MANAGEMENTKOMPASS
03 / 2021

Quanten-computing

F.A.Z.-INSTITUT

sopra steria

Frédéric Munch
Vorstand
Sopra Steria

„Quantencomputing wird in Zukunft zu den zentralen Grundlagentechnologien zählen und gewinnt schon heute in Schlüsselbereichen der deutschen Wirtschaft an Relevanz. Längst gibt es mehr Mitspieler auf dem Markt als nur die großen Player aus den USA. Stellen wir jetzt die Weichen richtig, hat Europa die Chance, sich als führender Standort zu etablieren."

Frank Weber
Entwicklungsvorstand
der BMW AG

„Quantencomputing ist eine wegweisende Zukunftstechnologie und hat erhebliches Potenzial für eine Vielzahl von Anwendungen – zum Beispiel in der Batteriezellchemie oder für das automatisierte Fahren."

Rory McLaren
Technology Strategist der Gruppe Deutsche Börse

„Quantencomputing bietet ein enormes Potenzial für die Kapitalmärkte in den Bereichen der Simulation, Optimierung, KI/ML und Kryptographie. Im Risikomanagement könnte diese Technologie beispielsweise eingesetzt werden, um die Einflüsse unterschiedlicher Parameter besser zu simulieren."

VORWORT

Die ersten kommerziell verfügbaren Quantencomputer zeigen, dass Quanteneffekte tatsächlich zur Lösung von Optimierungsaufgaben und Simulationen geeignet sind. Die Einsatzmöglichkeiten sind noch sehr begrenzt und die Fehlerquoten hoch, doch Forscher und Unternehmer insbesondere aus den USA, Europa und China arbeiten intensiv an der Weiterentwicklung der Quantentechnologie. Deutsche Forscher könnten sich dank großzügiger staatlicher Unterstützung bald einen Spitzenplatz unter den Entwicklern von Quantencomputern sichern. Schon jetzt tragen Grundlagenforschung und Zulieferteile aus Deutschland auch zum Erfolg US-amerikanischer Quantencomputer bei.

Außerhalb der Quantenforschung stehen Unternehmen vor der Aufgabe, Anwendungen und Geschäftsmodelle für Quantencomputing zu entwickeln. Einige Branchen sind hier Vorreiter wie Chemie und Pharma, Automobil, Logistik und Finanzdienstleistungen. Unternehmen, die in die Quantentechnologie investieren, gestalten die technologische Entwicklung mit und sichern sich Wettbewerbsvorteile.

Doch von Quantencomputing gehen neben Chancen auch Risiken aus: So lassen sich mit leistungsfähigen Maschinen wahrscheinlich auch einige herkömmliche kryptographische Verfahren aushebeln. Doch auch hierfür entwickeln Forscher bereits neue Lösungen.

Sopra Steria
F.A.Z.-Institut

EXECUTIVE SUMMARY

Keine Science-Fiction mehr

Die Leistungsfähigkeit von Quantencomputing steigt und eröffnet für die Zukunft neue Wettbewerbsvorteile für Branchen wie Logistik, Automobil, Chemie, Pharmazie, Materialforschung und Finanzen. Aber auch Unternehmen und Verwaltungen, für die Datensicherheit essenziell ist, sollten sich mit der Technologie jetzt schon beschäftigen.

1. Vorbereitet sein ist alles: Unternehmen und Verwaltungen sollten die Entwicklung im Quantencomputing generell und speziell in ihren eigenen Branchen oder Fachbereichen genau verfolgen. Für einige Branchen und Aufgaben wird Quantencomputing auf lange Sicht zwar relevanter sein als für andere. Doch das Thema Post-Quantum-Kryptographie könnte schon in wenigen Jahren viele Organisationen betreffen.

Es gibt zwar heute noch keine praxistauglichen Quantencomputer, die bei der Lösung alltäglicher Aufgaben von Unternehmen und Verwaltungen klassischen Computern überlegen sind. Doch die Entwicklung auf diesem Gebiet schreitet schnell voran. Experten erwarten einen Durchbruch bereits innerhalb der kommenden zehn Jahre. In manchen Branchen dürfte Quantencomputing dann zu einem Wettbewerbsvorteil werden. Dazu gehören vor allem Logistik, Telekommunikation, Chemie, Materialentwicklung und Ingenieurswesen, Medizin und Pharma, Finanzdienstleistungen und IT-Sicherheit.

Neben den Chancen bringt Quantencomputing aber auch neuartige Risiken, zum Beispiel in Bezug auf herkömmliche Verschlüsselungsverfahren. Gerade öffentliche Verwaltungen und Finanzdienstleister sollten die Entwicklungen im Quantencomputing auch unter Sicherheitsaspekten verfolgen.

2. Quantencomputing wird anfangs nur für spezielle Aufgabenstellungen geeignet sein. Dazu gehören Optimierungsberechnungen für komplexe Systeme sowie Simulationen von Szenarien, Molekülen und chemischen Prozessen. Es sollte deshalb geprüft werden, ob diese Art von Aufgaben für die eigene Organisation relevant ist.

Qubits können im Vergleich zu ihrem klassischen Analogon – den Bits – viel mehr Information gleichzeitig repräsentieren und somit in jeder Rechenoperation mehr Daten verarbeiten. Für viele Anwendungen ergeben sich so stark beschleunigte Algorithmen. Statt Jahre auf klassischen Computern benötigen Quantencomputer nur Sekunden.

So lassen sich Wetterprognosen und Finanzrisikomodelle mit Hilfe von Quantencomputern mit wesentlich mehr Parametern rechnen als mit klassischen Computern und das sogar in Echtzeit. Machine Learning und Künstliche Intelligenz gewinnen durch Quantencomputing drastisch an Leistungsfähigkeit. Auf diese Weise können große Datenbestände verarbeitet werden, um Muster in Daten aufzuspüren, wobei mehrere Lösungswege gleichzeitig berechnet werden können. Selbst bislang unlösbare, da sehr komplexe Probleme könnten in Zukunft mit Quantenalgorithmen angegangen werden. Dazu gehören möglicherweise auch der Klimawandel oder bislang unheilbare Krankheiten.

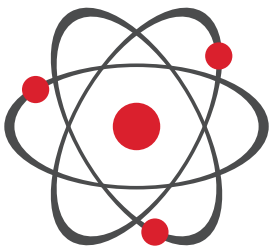
3. Der Zugriff auf Quantencomputer wird vor allem in der Anfangszeit über die Cloud angeboten werden. Schon heute betreiben nordamerikanische Unternehmen Quanten-Clouds, die zur Forschung oder für praktische Erfahrungen mit Quantencomputing genutzt werden können – auch von Unternehmen. Ein Test lohnt sich, um die eigene IT-Abteilung mit der neuen Art von Algorithmen vertraut zu machen.
Quantencomputer dürften auch in Zukunft vor allem in Hybridlösungen eingesetzt werden, um bereits existierende Informationstechnologie zu ergänzen. Für einfache Aufgaben wird herkömmliche Hard- und Software weiterhin besser geeignet sein. Heutige Computer haben den großen Vorteil, dass sie zuverlässig funktionieren und robust sind. Quantencomputer sind dagegen technisch sehr aufwendig und sensibel. Vieles erinnert an die Anfangszeiten der klassischen Informationstechnologie.

Die bisherigen Quantum-Cloud-Angebote sind zwar Ready-to-Use-Lösungen, doch ohne Kenntnisse in Quantencomputing kaum von Unternehmen und Verwaltungen nutzbar. Dafür sind Mitarbeiter erforderlich, die anstehende Aufgaben auch auf mathematischer und physikalischer Ebene durchdringen. Ein klassisches Informatikstudium genügt dafür nicht. Es gibt mittlerweile bereits erste Quantencomputing-Angebote von Universitäten und Fachhochschulen auch in Deutschland.

4. Bei der Verschlüsselung von Daten leitet Quantencomputing einen Paradigmenwechsel ein. Forscher arbeiten derzeit an neuen Standards für eine Post-Quanten-Kryptographie. Denn ein Großteil der heute eingesetzten asymmetrischen kryptographischen Verfahren kann nicht mehr als sicher betrachtet werden, wenn Quantencomputer einmal leistungsfähig genug sind.
Eine Lösung verspricht die Post-Quanten-Kryptographie. Dazu werden quantenresistente Algorithmen auf klassischen IT-Plattformen implementiert. Wie heutige Algorithmen gründen sie Sicherheit auf mathematische Komplexität, aber mit anderen Verfahren. Das BSI hat im Hochsicherheitsbereich bereits mit der Migration zur Post-Quanten-Kryptographie begonnen. Es steht ein zum Schutz von Verschlusssachen bis zum Einstufungsgrad „Geheim" zugelassenes Produkt zur Verfügung, das ein Post-Quanten-Verfahren zur Schlüsselverteilung umsetzt.

Doch bis Post-Quanten-Kryptographie zum Standard wird, könnten noch Jahre vergehen. Unternehmen und Verwaltungen, die vertrauliche Daten über öffentliche Netze verbreiten und mit asymmetrischen oder hybriden kryptographischen Verfahren verschlüsseln, sollten dennoch aktiv werden. Denn heute von Hackern erbeutete Daten können in Zukunft möglicherweise entschlüsselt werden. Um die Bedrohung zu begrenzen, sind Datenvermeidung und Datensparsamkeit zu empfehlen. Insbesondere der Umfang der Übertragung vertraulicher Daten über öffentliche Netze sollte hinterfragt werden. Outsourcing oder Cloud-Nutzung sind ebenfalls erwägenswert. Dazu gehört auch, Redundanzen in der Datenhaltung aufzulösen, die Speicherdauer zu begrenzen und sichere Löschverfahren zu verwenden. Ein zweiter Ansatz ist, die Hürde für das Entschlüsseln von Daten bereits mit heutiger Technologie möglichst hoch zu setzen. «

kurz & knapp



35 Prozent
der Unternehmen und Verwaltungen halten Quantencomputing für die eigene Branche für relevant.

Quelle: Potenzialanalyse „Quantencomputing" (Sopra Steria), 2021

TREND

Quanten-computing kommt

Die Entwicklung im Quantencomputing schreitet weltweit schnell voran. Derzeit gibt es zwar noch keine Maschine, die klassischen Computern bei unternehmens- oder verwaltungsrelevanten Aufgaben überlegen wäre. Dies dürfte sich aber in absehbarer Zeit ändern.

Im September 2021 hat IBM den Bau eines Quantencomputers mit über 1.000 Qubits bis Ende 2023 angekündigt. Dies ist ein großer Schritt in Richtung praxisrelevante Quantenrechner. Der Quantencomputer, der in diesem Jahr in Ehningen bei Stuttgart aufgestellt wurde, hat lediglich 27 Qubits. Theoretisch verdoppelt ein Quantencomputer mit jedem zusätzlichen Qubit seine Leistungsfähigkeit. Deshalb gelten 1.000 Qubits für diese Technologie als viel. In dieser Größenordnung lassen sich bereits wirtschaftlich interessante Berechnungen durchführen, sagt auch Arne Schönbohm, Direktor des BSI, gegenüber dem „Managementkompass“. Allerdings sind Qubits beim heutigen Stand der Technik noch sehr instabil und können nur für kurze Zeitfenster für Berechnungen genutzt werden. Auch die Fehlerquoten sind extrem hoch. An der Fehlerkorrektur arbeiten die Forscher deshalb intensiv.

Neben IBM arbeitet eine Reihe weiterer Unternehmen an skalierbaren Quantencomputern. Google präsentierte Ende 2019 einen Quantencomputer mit 53 Qubits und demonstrierte damit schon die Überlegenheit gegenüber einem klassischen Computer – allerdings bei einer sehr speziellen Fragestellung. Eine Weiterentwicklung bis 1.000 Qubits ist bis 2029 geplant. Mitte 2021 hat auch Amazon seinen Einstieg in die Quantencomputerentwicklung angekündigt. Weitere Hersteller sind Honeywell und Ionq, die allerdings nicht auf die verbreitete Supraleitertechnologie, sondern auf Ionenfallen setzen. Daneben stellt D-Wave-Systems aus Kanada Quantencomputer für spezielle Optimierungsaufgaben her, sogenannte Quantum Annealer.

Außerhalb Nordamerikas kann China erste Erfolge mit einem Quantencomputer vorweisen. Dort demonstrierte die University of Science and Technology of China Ende 2020 in einem ebenfalls sehr speziellen Experiment dessen Überlegenheit gegenüber klassischen Computern.

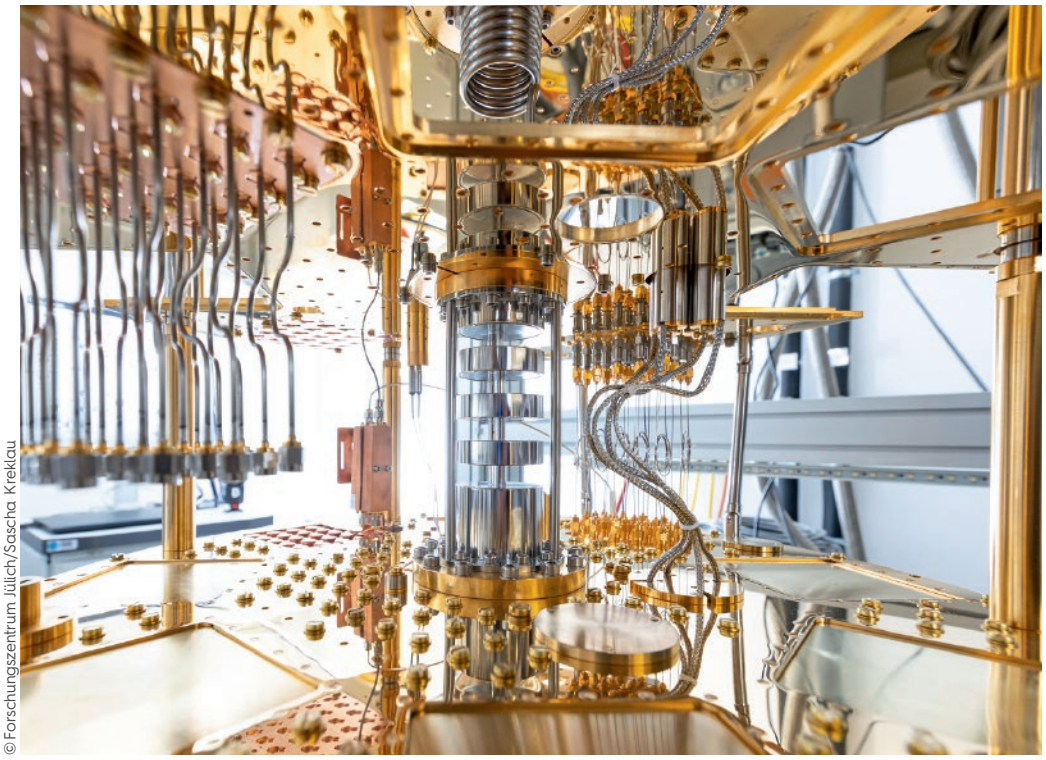
Jetzt steht auch Deutschland in den Startlöchern. Für 2022 hat das Forschungszentrum Jülich den ersten europäischen Quantencomputer angekündigt mit voraussichtlich rund 50 Qubits. Die Bundesregierung hat im Rahmen ihres Konjunkturprogramms im Mai 2021 insgesamt 2 Milliarden Euro für die Entwicklung von Quantencomputern genehmigt. Damit sollen in den kommenden fünf Jahre zwei leistungsstarke Quantencomputer inklusive Software gebaut und ein Ökosystem mit Anwendern aus Forschung und Wirtschaft eingerichtet werden.

Quantenbits aus der Cloud

Klar ist schon jetzt, dass sich zunächst nur wenige Anwender einen eigenen Quantencomputer ins Rechenzentraum stellen werden. Wobei es durchaus Ausnahmen in forschungsintensiven Branchen geben wird. So hat die US-amerikanische Cleveland Clinic gerade einen eigenen Quantencomputer für Forschungszwecke für 2022 bestellt. Für die Mehrheit der Nutzer dürften in naher Zukunft aber nur Cloud-Lösungen in Frage kommen. Quantencomputer werden wohl auch vor allem in Kombination mit klassischen Rechnern, also hybrid, eingesetzt werden, um die Vorteile beider Systeme zusammenzuführen.

> „Wer Quantentechnologien anwenden kann, wird sich maßgebliche Wettbewerbsvorteile sichern.“
>
> *Achim Berg*

Es gibt bereits Cloud-Angebote für Quantencomputing. Microsoft etwa bietet über



© Forschungszentrum Jülich/Sascha Kreklau

Das Forschungszentrum Jülich arbeitet derzeit am ersten europäischen Quantencomputer. Er soll 2022 in Betrieb gehen. Hier ein Blick ins Labor.

das Ökosystem Azure Quantum Anwendern Zugang zu entsprechenden Rechnern. Und mit Amazon Braket hat Amazon ebenfalls einen Cloud-Dienst für Quantencomputer.

IBM setzte von Anfang an auf die Cloud. Der IBM Q System One in Ehningen ist Teil des bundesweiten Fraunhofer-Kompetenznetzwerks Quantencomputing, das Forschern und Unternehmen die Nutzung über die Cloud ermöglicht. Das Netzwerk unterstützt Unternehmen dabei, Fachkompetenz für Quantencomputing aufzubauen und erste praktische Erfahrungen zu sammeln.

Die angeschlossenen Forschungsinstitute arbeiten unter anderem daran, Quantencomputing für das Design neuer Materialien und zur Simulation quantenchemischer Reaktionen einzusetzen sowie Quantenalgorithmen für Optimierungen zu entwickeln. Zu den Anwendungsgebieten zählen die Modellierung von Batterien und Brennstoffzellen, Stabilitätsanalysen kritischer Infrastrukturnetzwerke sowie Anwendungen und Algorithmen für Fertigung, Entwicklung, Logistik, Energie und Finanzwesen.

Großes Potenzial

Laut einer Umfrage des Digitalverbands Bitkom von April 2021 sieht die Mehrheit der Unternehmen in Deutschland in Quantencomputing einen Wettbewerbsfaktor für die Zukunft. Unter den befragten mehr als 600 Entscheidern schreibt mehr als die Hälfte der neuen Technologie eine große Bedeutung für die Wettbewerbsfähigkeit der deutschen Wirtschaft zu.

Bitkom-Präsident Achim Berg hebt hervor: „Wer Quantentechnologien beherrschen und anwenden kann, wird sich maßgebliche Wettbewerbsvorteile sichern. Quantencomputer können Probleme lösen, an denen Superrechner scheitern, etwa die Berechnung komplexer Liefer- und Produktionsketten, die Simulation der Wirksamkeit von Medikamenten im Körper oder die Analyse und Prognose von Entwicklungen an den Finanzmärkten."

Die Fraunhofer-Allianz Big Data und KI hat im August 2021 eine Studie zu „Quantum Machine Learning" herausgegeben. Verfahren der Künstlichen Intelligenz und des maschinellen Lernens lassen sich demnach für Quantencomputer so anpassen, dass sie mehrere Lösungswege gleichzeitig beschreiten können.

So können Quantencomputer große Datenbestände in einem einzigen Schritt verarbeiten, Muster in Daten aufspüren, die klassische Computer nicht entdecken, und auch aus unvollständigen oder unsicheren Daten relativ verlässliche Ergebnisse liefern. Der Studie zufolge könnte KI durch das Quantencomputing gerade in Branchen wie Materialforschung, Medizin, Logistik, Finanzen und IT Security einen mächtigen Schub erfahren. «

Eric Czotscher
ist Leitender Redakteur research im F.A.Z.-Institut.
e.czotscher@faz-institut.de

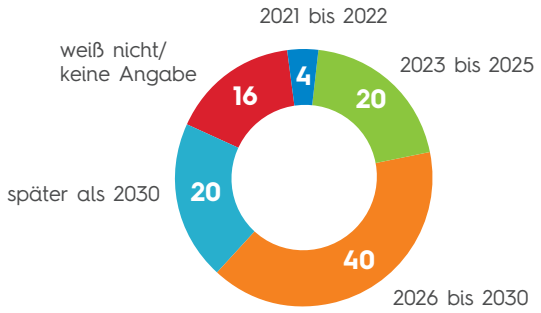
POTENZIALANALYSE

Quantencomputing als reale Option ab 2026 eingestuft

Für die Potenzialanalyse „Quantencomputing" von Sopra Steria hat F.A.Z. Business Media | research 158 Entscheiderinnen und Entscheider aus Unternehmen und öffentlichen Verwaltungen zur Relevanz und zu den möglichen Einsatzgebieten von Quantencomputing befragt.

In fünf Jahren spürbare Effekte erwartet

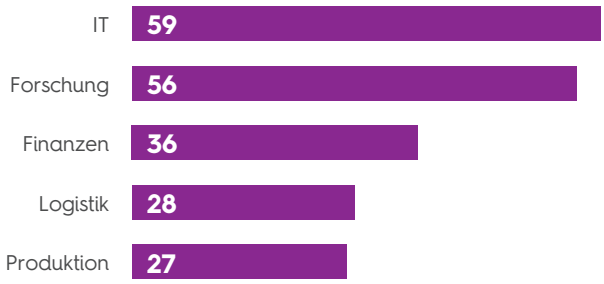
Antwort auf die Frage: „Wann wird der Einfluss von Quantencomputing auf Ihr Unternehmen/Ihre Verwaltung voraussichtlich spürbar werden?"; in Prozent der Befragten



Kurzfristig erwarten die Befragten nicht, dass sich Quantencomputing auf die eigene Organisation auswirken wird, mittelfristig dagegen schon. 40 Prozent rechnen bereits für 2026 bis 2030 mit spürbaren Effekten.

IT und Forschung im Fokus

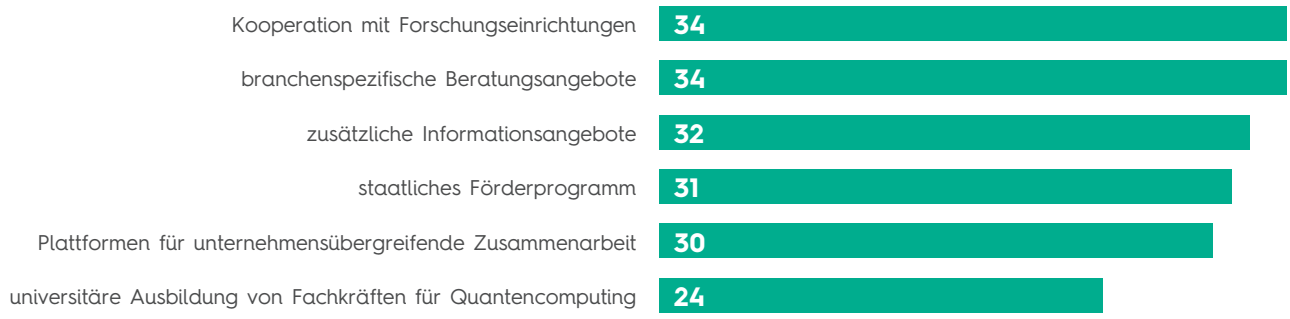
Antwort auf die Frage: „Für welche Bereiche könnte Quantencomputing in Zukunft relevant werden?"; in Prozent der Befragten



Wenn sich Quantencomputing durchsetzt, dann wird dies am ehesten die Organisationsbereiche IT und Forschung betreffen. Aber auch der Finanzbereich inklusive Controlling wird die neuen Möglichkeiten der Technologie nutzen, wie viele Befragte vermuten.

Kooperation mit Forschern gesucht

Antwort auf die Frage: „Welche der folgenden Angebote wären für Ihre Organisation hilfreich, um das Potenzial von Quantencomputing zu nutzen?"; in Prozent der Befragten



Unternehmen und Verwaltungen wünschen sich vor allem Forschungskooperationen, um sich mit Quantencomputing vertraut zu machen. Aber auch branchenspezifische Angebote sowie Plattformen für eine unternehmensübergreifende Zusammenarbeit wären willkommen, um das Potenzial von Quantencomputing in der eigenen Organisation ausschöpfen zu können.

Quelle: Potenzialanalyse „Quantencomputing" (Sopra Steria), 2021

THINK TANK

Quantencomputer eignen sich besonders dafür, komplizierte Optimierungsprobleme mit vielen Einflussfaktoren und Verknpüfungen zu lösen, beispielsweise in der Logistik.

Quantencomputer als schnelle Optimierer

Die besonderen Eigenschaften von Quantencomputern im Vergleich zu klassischen Computern machen sie zu besseren Problemlösern für bestimmte Fragestellungen. Dazu gehören Optimierungen und Simulationen in Logistik, Finanzwirtschaft und Materialforschung. Erste Algorithmen existieren bereits, aber die Hardware entwickelt sich erst.

Ein klassisches Bit ist ein Objekt, das die beiden Werte 0 oder 1 annehmen kann. Physikalisch kann dieses Objekt ein elektronisches Bauteil sein, vorstellbar ist aber auch ein Uhrzeiger, der waagerecht oder senkrecht steht. Klassische Bits haben zwei zentrale Eigenschaften, die so selbstverständlich sind, dass sie nur genannt werden, wenn von Quantencomputing die Rede ist: Erstens ist der Wert eines Bits zu jedem Zeitpunkt der Berechnung eindeutig definiert. Dieser Wert kann gemessen werden, und die Messung ändert den Wert des Bits nicht.

Zweitens verändert sich der Wert an einem Bit nicht automatisch, wenn sich der Wert an einem anderen Bit ändert. Es braucht eine – wenn auch oft sehr kurze – Zeitspanne, bis die Änderung an einem Bit »

sich an einem anderen Bit auswirkt – zumindest die Zeit, die Licht benötigt, um den Raum zwischen beiden Bits zu überwinden.

Das Besondere an Quantenbits

Ein Quantenbit (Qubit) ist demgegenüber ein Objekt, das die beiden Werte 0 oder 1 oder Werte dazwischen annehmen kann. Physikalisch kann dieses Objekt zum Beispiel ein gefangenes Ion, eine supraleitende Schlaufe oder ein polarisiertes Lichtteilchen sein. Man kann sich aber auch den Zeiger einer Uhr vorstellen, der waagrecht oder senkrecht oder irgendwo dazwischen stehen kann.

> „Optimierungs- und Simulationsprobleme kommen praktisch überall vor.“

Für Quantenbits gelten außerdem die seltsamen Gesetze der Quantenphysik: Erstens verändert der Messvorgang den Zustand des Quantenbits. Wird ein Quantenbit gemessen, so nimmt es definitiv den Zustand 0 oder 1 an, also wie ein klassisches Bit, und gibt dieses Ergebnis entsprechend aus. Es verhält sich damit beispielsweise wie ein Photon, das einen Polarisationsfilter entweder passiert oder nicht passiert und so die Polarisation des Filters annimmt.

Zweitens gibt es das Phänomen der Quantenverschränkung. Das bedeutet, dass die Messung eines Quantenbits unmittelbar die Eigenschaften eines anderen Quantenbits verändern kann. Diese Veränderung erfolgt mit Überlichtgeschwindigkeit; nachgewiesen ist mehr als die zehntausendfache Lichtgeschwindigkeit. Dieser Effekt ist so verblüffend, dass Einstein ihn „spukhafte Fernwirkung“ nannte.

Anwendungsbereiche: Quantenoptimierung und Quantensimulation

Optimierungs- und Simulationsprobleme kommen praktisch überall vor: In der Logistik, bei der Optimierung von Produktionsprozessen und Verwaltungsabläufen, bei der Simulation von betriebswirtschaftlichen oder finanzwirtschaftlichen Situationen und bei der Entwicklung neuer Arzneimittel und Materialien. Weitere Optimierungsaufgaben betreffen die Künstliche Intelligenz und damit den gesamten Bereich der Mustererkennung in großen Datenbeständen.

Solche Optimierungsaufgaben sind bei einer großen Zahl von Einflussfaktoren sowie bei vielen Abhängigkeiten zwischen diesen

Welches ist die effizienteste Route zur Auslieferung von Paketen? Quantencomputer können dieses „Problem des Handlungsreisenden“ künftig schneller lösen.

Faktoren auf klassischen Computern nur bis zu einem gewissen Grad zu berechnen.

Quantencomputer versprechen hier Abhilfe. Denn Quantenalgorithmen können wegen der Verschränkung von Quantenbits systemisch arbeiten: Ein Quantenalgorithmus bereitet ein System von Quantenbits für eine Problemstellung vor und lässt dann der Natur ihren freien Lauf. Dieser selbst laufende Prozess sorgt dafür, dass alle Abhängigkeiten berücksichtigt werden und am Ende eine für das System – und damit für die Problemstellung – sehr gute Lösung herauskommt.

Algorithmen existieren bereits

Wer einmal Marketingmaßnahmen entworfen oder gruppendynamische Prozesse gesteuert hat, hat im Sinne von Quantenalgorithmen gedacht. Auch bei solchen Optimierungen geht es darum, die Beziehungen oder „Verschränkungen" von Personen untereinander zu nutzen, um das System effizient in einen guten Zustand zu bringen. Was „gut" ist, hängt bei der Problemstellung von der Intention des Nutzers ab. In der physikalischen Übersetzung bedeutet es meistens den Zustand niedrigster Energie.

Die Funktionsweise von Quantenoptimierung und -simulation wird aus algorithmischer Sicht heute bereits gut verstanden. Aktuell fehlt es aber noch an der geeigneten Hardware, um Probleme einer nennenswerten Größenordnung auf Quantencomputern zu rechnen. Denn Quantenbits sind extrem empfindlich und fehleranfällig.

Aktuelle Quantenhardware kann für praktische Anwendungen bisher noch keine Probleme lösen, die nicht jede Rechen-App auf einem Handy ebenfalls lösen könnte. Aber beispielsweise IBM, Google, Amazon und D-Wave sowie chinesische, europäische und deutsche Initiativen arbeiten daran, leistungsfähige Hardware auf den Markt zu bringen.

Quantenkommunikation einfacher umsetzbar

Bei der Quantenkommunikation müssen nicht alle Quantenbits gleichzeitig arbeiten, sondern sie können nacheinander angesteuert und verarbeitet werden. Das macht die Quantenkommunikation hardwareseitig einfacher, und sie ist auch heute schon nutzbar.

> „Unternehmen und Verwaltungen werden nicht einfach auf den Zug aufspringen können."

Quantenbits ändern ihren Wert, wenn man sie misst. Dieser Effekt dient in der Quantenverschlüsselung dazu, Lauscher bei einem Datentransport zu entlarven. Falls ein Lauscher einen Quantenkanal, zum Beispiel ein Glasfaserkabel, anzapft, ändern die darin befindlichen Quantenbits ihren Zustand: Ein belauschtes Quantenbit erhält den Wert 0 oder 1. Der Lauscher kann aber nicht wissen, wie der Zustand vorher war. Er kann das Quantenbit also auch nicht unverändert weiterschicken.

Nur der rechtmäßige Sender kennt den ursprünglichen Zustand des Quantenbits. Auf diesem Wissensvorsprung basieren Verfahren zur abhörsicheren Kommunikation mit Quantenbits.

Telekommunikationsunternehmen sind heute dabei, die Hardware für die Quantenverschlüsselung zu bauen und zum Einsatz zu bringen. Anwender der Telekommunikation können Dienstleistungen für den Datentransport bereits nutzen.

Jedes Unternehmen muss aber künftig noch mehr darauf achten, dass die eigenen sensiblen Daten gut verschlüsselt gelagert werden. Denn Quantencomputer der Zukunft werden womöglich heutige Verschlüsselungsverfahren zur Datenlagerung brechen können. Anbieter für Datenlagerung sind bereits dabei, sich auf diesen Fall vorzubereiten.

Quantum Readiness

Quantencomputing hat ein hohes disruptives Potenzial, sobald Quantenhardware verfügbar ist. Allerdings werden Unternehmen und Verwaltungen dann nicht einfach auf den Zug aufspringen können. Es lohnt sich deshalb, bereits jetzt einen Blick auf die Prozesse des eigenen Unternehmens oder Bereichs zu werfen, um zu erkennen, ob es mögliche Anwendungsbereiche gibt. Ein Sachbearbeiter wird in absehbarer Zeit von den Besonderheiten des Quantencomputings kaum etwas merken, aber die IT-Abteilung sollte sich damit auseinandersetzen und entsprechendes Know-how aufbauen. «

© Just

Prof. Dr. Bettina Just lehrt und forscht in Mathematik und Informatik an der Technischen Hochschule Mittelhessen THM. Sie ist Organisatorin des Netzwerkes „Quanten an Hochschulen für angewandte Wissenschaften" und Leiterin des Kompetenzzentrums Quantencomputing der TransMIT GmbH.

managementkompass@faz-institut.de

THINK TANK

Europäischer Quantencomputer ab 2022

Bislang hat Deutschland keinen Quantencomputer entwickelt. Hiesige Wissenschaftler holen bei der angewandten Forschung aber auf. In Jülich soll bereits 2022 die erste europäische Maschine präsentiert werden, stellt Prof. Dr. Frank Wilhelm-Mauch, Direktor des Instituts für Quantum Computing Analytics am Forschungszentrum Jülich, im Interview in Aussicht.

Herr Professor Dr. Wilhelm-Mauch, wo steht Deutschland beim internationalen Wettbewerb im Quantencomputing?
Der eigentliche Wettbewerb findet derzeit noch mit der Natur statt: Wird es uns Menschen gelingen, ihr einen praxistauglichen Quantencomputer abzuringen, der skalierbar ist und zur Lösung realer Aufgaben verwendet werden kann? Wir bewegen uns hier auf unbekanntem Terrain ohne festgelegten Fahrplan. Es ist auch noch nicht entschieden, welche physikalische Plattform für Quantencomputer am besten geeignet ist.

> „Deutschland holt bei der angewandten Forschung auf."

Deutschland gilt dabei als Geheimfavorit, seit hiesige Forscher den entscheidenden Schritt von der Grundlagen- in die anwendungsnahe Forschung getan haben. In einer Reihe internationaler Forschungsteams zum Beispiel in den USA spielen deutsche Experten schon länger eine zentrale Rolle. Hier in Jülich arbeiten wir am ersten europäischen Quantencomputer „OpenSuperQ".

Forscher weltweit entwickeln unterschiedlichen Plattformen. Was sind die Favoriten?
Die aussichtsreichsten Systeme für einen praxistauglichen Quantencomputer sind Supraleiter, Ionenfallen und Atomfallen für neutrale Atome. IBM und Google arbeiten mit Supraleitern. Deutschland steuert dazu viele Komponenten bei. Auch bei OpenSuperQ wird diese Technik verwendet. Die Universität Innsbruck und die Unternehmen Infineon und Honeywell experimentieren mit Ionenfallen. Derzeit wecken auch Fortschritte bei Atomfallen mit neutralen Rydberg-Atomen Hoffnung. Prof. Dr. Immanuel Bloch vom Max-Planck-Institut für Quantenoptik arbeitet auf Basis von Rydberg-Atomen gemeinsam mit französischen Partnern an einem frei programmierbaren Quantencomputer.

In welchen Bereichen ist Deutschland auf Augenhöhe mit Wettbewerbern?
Deutschland ist führend bei der Grundlagenforschung und holt nun auch bei der angewandten Forschung auf. Deutsche Forscher waren bislang zwar gut darin, einzelne Bauteile immer weiter zu perfektionieren. Doch was fehlte, war ein Team, das alle Komponenten zu einem Quantencomputer zusammenbaut.

Das Förderprogramm der Bundesregierung für einen Demonstrations-Quantencomputer dürfte hier für Schub sorgen. So kann Deutschland in die Rolle eines Systemintegrators hineinwachsen. Das Walther-Meißner-Institut der Bayerischen Akademie der Wissenschaften hat vom Bundesministerium für Bildung und Forschung (BMBF) eine Förderung von 14,5 Millionen Euro erhalten, um innerhalb von vier Jahren einen Prototyp für einen Quantencomputer basierend auf supraleitenden Qubits zu bauen. Neuer Direktor des Instituts ist Prof. Dr. Stefan Filipp,

Prof. Dr. Frank Wilhelm-Mauch
ist Direktor des Instituts für Quantum Computing Analytics am Peter Grünberg Institut des Forschungszentrums Jülich und Inhaber einer Professur für Theoretische Physik an der Universität Saarbrücken.

> „Quanten-Big-Data oder Giga-Qubits werde ich wohl nicht mehr erleben.“

der zuvor bei IBM geforscht hat. Ein weiteres Beispiel ist das Verbundprojekt „Q-Ryd-Demo“, das vom BMBF mit 9 Millionen Euro unterstützt wird. Weitere 1,1 Millionen Euro fließen von Industriepartnern.

Der erste Quantencomputer in Deutschland steht in Ehningen: der „IBM Q System One“. Was für eine Maschine ist das?
Es handelt es sich um einen Quantencomputer mit 27 Qubits in supraleitenden, extrem tiefgekühlten Schaltkreisen. Er ist zwar einem klassischen Computer nicht überlegen, eignet sich aber dazu, Erfahrungen zu sammeln. Die Quantenüberlegenheit zeigt sich frühestens bei über 50 Qubits. Dann lässt sich die Rechenleistung eines Quantencomputers nicht mehr mit einem Supercomputer simulieren. Google hat einen Quantencomputer mit 53 Qubits und die chinesische Akademie der Wissenschaften mit über 60 Qubits entwickelt. Es handelt sich um wissenschaftliche Großgeräte für Laborversuche, die sich noch nicht für praktische Anwendungen eignen – auch wegen der hohen Fehlerquote.

Wie ist der Stand des europäischen Flaggschiff-Projekts OpenSuperQ in Jülich?
Das EU-geförderte Projekt läuft bis 2022. Das Ziel von 100 Qubits wird zwar nicht erreicht werden, aber 50 Qubits sind möglich. Mitte kommenden Jahres wollen wir den ersten europäischen Quantencomputer mit Software-Stack präsentieren und Komponenten aus Finnland, der Schweiz, Schweden, Spanien und Deutschland. Es handelt sich um ein Open-Source-Projekt, das für alle Nutzer offen ist. Seit September 2021 haben wir mit Prof. Dr. Rami Barends von Googles Quanten-Lab für KI prominente Verstärkung.

Welche Rolle spielen Unternehmen bei der Entwicklung von Quantencomputern?
Große Unternehmen wie VW, Daimler, BASF, Zeiss, E.ON oder Bayer haben Quanten-Forschergruppen und kooperieren kostenpflichtig mit Hardwareherstellern und Software-Start-ups. Zudem organisieren sich Firmen in Interessengruppen wie der Quantum Computing Industry Group in Deutschland oder dem Quantum Industry Consortium (QuIC) in Europa. Für IBM in Ehningen übernimmt die Fraunhofer-Gesellschaft die Koordination, um Universitäten und kleinen Unternehmen den Zugang zu erleichtern. Ein ähnliches Projekt plant die Plattform JUNIQ gemeinsam mit D-Wave in Jülich. JUNIQ bietet über Cloud-Dienste bereits Zugang zu Supercomputern an.

Wann rechnen Sie mit der kommerziellen Nutzung von Quantencomputing?
Das lässt sich nicht genau vorhersagen. Ich gehe davon aus, dass in den kommenden zehn Jahren erste Quantencomputeranwendungen zur Entwicklung neuer Materialien auf den Markt kommen werden. Der nächste Schritt könnten KI-Anwendungen für logistische Optimierungen in Echtzeit sein. Quanten-Big-Data oder Giga-Qubits werde ich wohl nicht mehr erleben. «

Das Interview führte Eric Czotscher.

PRAXIS

Erste Cloud-Angebote

Künftig werden Cloud-Dienstleister Unternehmen und Verwaltungen an ihre Quantencomputer-Farmen anbinden. Erste Cloud-Angebote gibt es bereits.

Auch in Zukunft werden wohl nur die wenigsten Unternehmen einen eigenen Quantencomputer nutzen. Das Produkt der Wahl ist vielmehr „Quantencomputing as a Serivce". Erste Angebote entstehen gerade – und erlauben einen Blick in die neue Welt.

An der Universität Innsbruck arbeitet ein Forscherteam bereits an der nächsten Generation von Quantencomputern für den massentauglichen Einsatz. Kompakt, modular und zu großen Teilen automatisiert sollen die Geräte sein. Eine erste Version, die in ein 19-Zoll-Serverrack passt, hat das Team eigenen Angaben zufolge bereits entwickelt. Dass sich künftig jedoch jedes Unternehmen einen eigenen Quantencomputer in den Serverraum stellen wird, ist unwahrscheinlich. Ein anderer Ansatz scheint besonders in der Anlaufphase des Quantencomputer-Zeitalters deutlich attraktiver: Quantencomputing as a Service.

Es ist wichtig zu verstehen, dass Quantencomputer nicht einfach schnellere oder besonders leistungsstarke Rechenmaschinen sind, sondern einen völlig anderen Ansatz verfolgen als alle bisherigen Computersysteme. So speziell wie der Ansatz der Rechner sind aber auch die Aufgaben, die Quantencomputer mit ihren Wahrscheinlichkeitsrechnungen lösen können.

Das führt dazu, dass sich in den kommenden Jahren oder sogar Jahrzehnten nur für wenige Unternehmen Investitionen in eigene Quantencomputer rechnen dürften. Denn die

> **„Nur für wenige Unternehmen rechnen sich Investitionen in eigene Quantencomputer."**

Systeme würden mit hohen Kosten für Anschaffung, Betrieb und Wartung zu Buche schlagen, wären aber nie völlig ausgelastet. Die gemeinsame Nutzung von Quantencomputern kann hingegen eine attraktive Alternative sein. Vernetzt über die Cloud-Infrastruktur, lassen sich die Dienste verschiedener Quantencomputer-Systeme als Container bereitstellen und nutzen. Die großen Hyperscaler bringen sich dafür bereits in Stellung.

Angebote für Experimentierfreudige

Unternehmen können sogar heute schon von Cloud-Angeboten profitieren. IBM Quantum System One – der erste Quantencomputer in Deutschland – ist mietbar. Gegen eine Monatsgebühr können Forschungseinrichtungen und Unternehmen gleichermaßen von dem System profitieren, das mit 27 Qubits zugleich das leistungsstärkste in Europa ist. Zur Einordnung: IBM-Großsysteme wie Condor sollen künftig mit 1.121 Qubits ein Vielfaches erreichen. Doch was es bis dahin braucht, sind unter anderem die passenden Anwendungen. Es ist also Zeit, um zu experimentieren.

Amazon AWS hat dafür den Dienst Amazon Braket ins Leben gerufen. Er erlaubt, Quantenalgorithmen zu entwickeln und in Simulationen zu testen, die die Rechenleistung der AWS-Cloud nutzen. Amazon arbeitet zudem mit den Quantencomputerherstellern Rigetti, Ionq und D-Wave zusammen, auf deren Plattformen sich die Algorithmen dann ausführen lassen.

Einen vergleichbaren Ansatz verfolgt Microsoft mit seinem Angebot Azure Quantum, das ebenfalls auf Quantenrechner von Ionq sowie von Honeywell zurückgreift. Google allerdings stellt, als dritter großer Hyperscaler, seine Quantencomputer-Simulation bislang noch nicht per Public Access bereit.

D-Wave selbst hat mit Leap einen Echtzeit-Quantum-Cloud-Service für Unternehmen entwickelt, der Zugriff auf dessen Rechner Advantage ermöglicht und vor allem für hybride Quantenanwendungen gedacht ist, die sowohl die Skalierbarkeit der Cloud als auch die Möglichkeiten des Quantencomputings nutzen. Die Besonderheit von D-Wave Advantage liegt darin, dass es sich anders als beim IBM-System nicht um einen universellen Quantencomputer handelt, sondern einen Annealing-Quantencomputer. Dieser macht sich Quanteneffekte zunutze und ist damit bei der Lösung sehr spezieller Probleme einem klassischen Computer gegenüber im Vorteil. Dazu gehören beispielsweise Optimierungs- oder auch Sortieraufgaben. Quantum Annealing gleicht darin hochspezialisierten Computerchips, die ausschließlich zur Lösung eines speziellen Problems geeignet sind.

Anbieter wie Fujitsu ermöglichen wiederum den Zugriff auf Simulationen des Quantencomputings beziehungsweise des Quantum Annealing, nicht aber auf die jeweiligen Systeme selbst.

> „Nutzer müssen die Aufgaben auch auf mathematischer und physikalischer Ebene durchdringen.“

Für viele Unternehmen geht es zunächst darum zu verstehen, wie Aufgaben beschaffen sein müssen, damit ein künftiger Quantencomputer-Einsatz sinnvoll ist. Die Simulationen, die sich die Rechenpower klassischer Supercomputer zunutze machen, haben also nicht den Anspruch, die Leistungsfähigkeit eines echten Quantencomputers zu simulieren, sondern wollen vor allem dessen spezielle Mechanik erfahrbar machen.

Neue Technologie erfordert neue Organisationen

Diese unterschiedlichen Angebote eint, dass sie einerseits zwar Ready-to-Use-Lösungen sind, andererseits aber die Organisation und personellen Ressourcen vieler Unternehmen herausfordern. Denn dafür sind Mitarbeiter erforderlich, die die Aufgaben auch auf mathematischer und physikalischer Ebene durchdringen, statt lediglich einen klassischen Informatik-Background zu haben. Nur so können sie abschätzen, wann sich der Zugriff auf den Quantencomputer-Service überhaupt lohnt.

Ausgestattet mit diesem Know-how, dürften wir schon bald eine Vielzahl neuer Unternehmen sehen, die mit „Quantencomputing as a Service“ die Geschäftsmodelle der Zukunft bauen. «

Florian Eulner
ist Head of Tech Domain Microsoft (Division Industries) bei Sopra Steria.
florian.eulner@soprasteria.com

PRAXIS

Chancen für die Logistik

Seit mehr als 4.000 Jahren werden in Logistik und Handel Maschinen zur Berechnung eingesetzt. Eine der ältesten ist der Abakus. In den vergangenen 60 Jahren haben Computer die Steuerung zahlreicher Prozesse übernommen. Mit dem Quantencomputing begründen wir gerade eine neue Ära.

Viele Logistikunternehmen arbeiten mit geringen Margen und kommen erst durch Skaleneffekte auf ihre Kosten. Vorteile gegenüber dem Wettbewerb werden heute maßgeblich durch optimale Abläufe, rechnergestützte Optimierungen sowie Künstliche Intelligenz erzielt. Deshalb spielen Fortschritte in der Computertechnologie für die Logistik eine wichtige Rolle.

Heuristiken zur Optimierung

Die Erfindung des Halbleitertransistors 1948 hat den klassischen Computer erst möglich gemacht. Inzwischen können Computer in einer Sekunde viele Milliarden Rechenoperationen durchführen. Dennoch kommen sie an ihre Grenzen, wenn riesige Berechnungen erforderlich sind.

Nehmen wir an, eine Zustelltour soll optimal zusammengestellt werden, um 100 Pakete in der idealen Reihenfolge zu liefern. Die Zahl der möglichen Reihenfolgevarianten beträgt 100! (100 Fakultät) Möglichkeiten. Das sind etwa $9{,}3 \times 10^{157}$ Vergleichsoperationen. Das überfordert jeden klassischen Computer.

Bei Hermes lösen wir das Problem jeden Tag zur Zufriedenheit der Paketempfängerinnen und -empfänger, wie es sicher jeder schon erlebt hat. Dazu zerlegen wir das Problem in kleine Teile und lösen diese Teilaufgaben mit einem Approximationsalgorithmus. Ein solcher Algorithmus macht nichts anderes als – auf besonders schlaue Weise – Varianten auszurechnen und zu vergleichen. Die jeweils schlechtere Variante wird verworfen. Mit dieser Heuristik ist es zwar nicht möglich, zur optimalen Liefertour zu kommen. Jedoch lässt sich mit reichlich Rechenleistung und etwas Rechenzeit ein gutes, praktikables Ergebnis erzielen.

Quantencomputing wird neue Dimension eröffnen

Wichtig zu verstehen ist, dass Quantencomputer nicht einfach nur die im Vergleich zur bekannten Technik schnelleren Rechner sind. Mit ihnen lassen sich vielmehr Aufgaben lösen, die bislang nur näherungsweise, gar nicht oder über Umwege gelöst werden konnten. So braucht ein Quantencomputer für die Berechnung der Zustelltour aus dem obigen Beispiel nur eine einzige Rechenoperation für die ideale Lösung, die mit klassischer Technik nie berechenbar sein wird.

Dies ist der Grund, weshalb wir uns bei Hermes mit Quantencomputing beschäftigen. Bislang haben wir mit den öffentlich zugäng-

© Hermes

Für die Optimierung der Paketauslieferung verspricht Quantencomputing enorme Fortschritte. Künftig werden die Fahrer voraussichtlich viel Zeit und viele Kilometer einsparen können.

lichen Angeboten experimentiert. Im nächsten Schritt geht es darum, unter Verwendung von umfangreichen Daten eine dauerhafte Installation zu schaffen, um die Umsetzungserfahrungen mit der neuen Technik und die Ergebnisse der Quantencomputerberechnungen mit dem heutigen klassischen Weg zu vergleichen. Dabei sprechen wir immer noch von Forschung.

Je besser die Ergebnisse werden, desto interessanter wird eine kommerzielle Nutzung. Dabei gehen wir davon aus, dass wir uns keinen Quantencomputer in das Rechenzentrum stellen werden, sondern die Rechenleistung künftig als Dienstleistung aus der Cloud beziehen können. Bis in diese Praxis, insbesondere bis zur Ablösung der augenblicklich bestehenden Berechnungsverfahren, ist es jedoch noch ein weiter Weg.

Andererseits sind in der Nutzbarmachung der Quantencomputer in den vergangenen beiden Jahren große Fortschritte festzustellen. Es gibt inzwischen Programmierwerkzeuge, die die Komplexität der Quantenwelt weitgehend vom Softwareentwickler fernhalten. Somit muss sich niemand mit den physikalischen Details der Maschinen beschäftigen.

Turbo für Künstliche Intelligenz

Mit dem Quantencomputing kann man auch Künstliche Intelligenz (KI) beschleunigen. Für diese Anwendungsfälle gibt es speziell gestaltete Quantencomputer. Das Ziel ist hier insbesondere das maschinelle Lernen. Voraussetzung für Machine Learning sind große Datenmengen, deren Eigenschaft bekannt ist, um zum Beispiel ein neuronales Netz zu trainieren. Das neuronale Netz lernt solange, bis es selbsttätig zuverlässig neue Datenpakete klassifizieren kann.

Modelle für komplexe Aufgaben sind ebenfalls komplex und somit auf klassischen Computern sehr rechenintensiv. Für die Klassifizierung von Myriaden von Daten versprechen die Quantencomputer große Vorteile. Jedoch liegt im Quantencomputing das Feld der KI im Vergleich zu Optimierungsaufgaben noch etwas zurück.

Innovationen ante portas

Für die kommenden Jahre sind deutliche Verbesserungen in der Technologie zu erwarten. Eine Innovation, die dazu führen wird, dass sich die Kosten für Beschaffung und Betrieb eines Quantencomputers deutlich verringern, wird den Durchbruch bedeuten. Doch auch dann wird es immer ein Nebeneinander von klassischen Computern mit ihren Quantengeschwistern geben.

Wir Logistiker sind klug beraten, die Entwicklungen der Quantencomputer im Blick zu behalten oder auch eigene Erfahrungen mit ihnen zu sammeln. Wer eine ideale Lösung der logistischen Leistungserbringung berechnen (und anwenden) kann, ist seinen Wettbewerbern klar überlegen. «

> „Ein Quantencomputer braucht für die Berechnung der Zustelltour nur eine Rechenoperation.“

Bert Woschkeit
ist Chief Information Officer der Hermes Germany GmbH.
managementkompass@faz-institut.de

PRAXIS

Q-Akteure in Deutschland

Das **FORSCHUNGS-ZENTRUM JÜLICH** entwickelt derzeit den ersten europäischen Quantencomputer, den „Open Super Q", im Rahmen eines EU-Projekts. Die Maschine soll Mitte 2022 präsentiert werden und hat voraussichtlich eine Leistungsfähigkeit von rund 50 Qubits. Im Rahmen eines Open-Source-Modells wird der Computer für Dritte über die Cloud erreichbar sein.

In Jülich ist auch das Projekt **JUNIQ** Jülicher Nutzer-Infrastruktur für Quantencomputing ansässig. Dieses will über die Cloud deutschen und europäischen Forschern und Unternehmen Zugang zu mehreren Quantencomputern bieten. Ein erster Vertrag wurde mit dem kanadischen Unternehmen D-Wave-System zur Nutzung von dessen Quantum Annealer geschlossen. JUNIQ berät die Nutzer auch.

Die Initiative **MQV** Munich Quantum Valley wurde von der bayerischen Landesregierung ins Leben gerufen, um München als europäischen Standort und Hub für Quantenwissenschaften und -technologien zu fördern. Ziel ist unter anderem die Ansiedlung von Start-ups für Quantencomputing.

Das **WALTHER-MEISSNER-INSTITUT** der Bayerischen Akademie der Wissenschaften in Garching bei München plant, innerhalb der kommenden vier Jahre einen deutschen Quantencomputer zu bauen. Dazu hat es eine Förderung des Bundesministeriums für Bildung und Forschung (BMBF) in Höhe von 14,5 Millionen Euro erhalten.

Der erste Quantencomputer in Deutschland befindet sich in Ehningen, in der IBM-Zentrale. Der „Q System One" mit 27 Qubits ist Kern eines bundesweiten Forschungs- und Unternehmensnetzwerks, das die **FRAUNHOFER-GESELLSCHAFT** orchestriert. Unternehmen und Forscher können ohne große Hürden über die Cloud auf den Quantencomputer zugreifen, somit erste Erfahrungen sammeln und sich auch untereinander austauschen.

An der Universität Stuttgart arbeitet ein Forscherteam ebenfalls an einem deutschen Quantencomputer. Dieser setzt auf Atomfallen statt auf Supraleitertechnologie. Diese Technologie gilt neben Ionenfallen als weiterer Kandidat für praxistaugliche Quantencomputer. In Stuttgart werden dafür neutrale Rydberg-Atome eingesetzt. Das Verbundprojekt **Q-RYD-DEMO** erhielt vom BMBF eine erste Förderung von 9 Millionen Euro. Weitere 1,1 Millionen Euro fließen von Industriepartnern.

Die Unternehmenskooperation **QUTAC** Quantum Technology and Application Consortium vereinigt große deutsche Unternehmen, die sich gemeinsam auf die Quanten-Zukunft vorbereiten. Dabei stehen Industrieanwendungen im Vordergrund. Dem Konsortium gehören BASF, BMW, Boehringer Ingelheim, Bosch, Infineon, Merck, Munich Re, SAP, Siemens und Volkswagen an.

PRAXIS

Finanzereignisse lassen sich mit Quantencomputern künftig in Echtzeit und mit zahlreichen Parametern analysieren und simulieren.

Bessere Risikomodelle für die Finanzbranche

Kreditinstitute und Versicherungen dürften von den Fortschritten im Quantencomputing besonders profitieren. Mögliche Anwendungsfälle sind stark verbesserte Risikomodelle und Szenarioanalysen, aber auch ein genaueres Kundendatenmanagement. Erste Projekte zeigen das große Interesse von Finanzdienstleistern an der neuen Technologie.

Kreditinstitute und andere Finanzdienstleister stützen ihre Geschäftsmodelle zunehmend auf das Datenmanagement. Gegenwärtig führt beispielsweise die Deutsche Bank täglich 600 Milliarden Rechenvorgänge allein zur Analyse von Markt- und Kreditrisiken durch. In absehbarer Zeit dürfte dieser Wert auf über 1 Billion steigen. Die Finanzwirtschaft könnte damit sehr von erheblich kürzeren Berechnungszeiten im Quantencomputing profitieren.

Außerdem eröffnet sich Finanzinstituten dank der neuen Technologie die Möglichkeit, komplexere Modelle zur Berechnung künftiger Entwicklungen an den Kapitalmärkten zu entwickeln. Heute ist die Zahl möglicher Parameter durch die Rechenzeit begrenzt. Quantencomputer dagegen können gleichzeitig mit viel mehr Faktoren arbeiten.

Börse testet komplexe Risikomodelle

Ein Pilotprojekt der Deutschen Börse mit dem Fintech JoS Quantum hat gezeigt, dass ein Quantencomputer die Berechnung von Risikomodellen außerordentlich beschleunigt. Solche Risikomodelle simulieren etwa die finanziellen Auswirkungen, die sich durch bestimmte makroökonomische Ereignisse ergeben. Heute verwendet die Börse dafür noch klassische Monte-Carlo-Simulationen auf Standardhardware. Die Risikoabschätzung ist dabei umso genauer, je mehr Simulationsparameter berücksichtigt werden. Doch mit der Komplexität des Berechnungsmodells erhöht sich die Rechenzeit exponentiell. So würde die Berücksichtigung von 1.000 Parametern die Rechenzeit auf Basis der derzeit verfügbaren IT-Infrastruktur auf mehrere Jahre hochschrauben.

Im Pilotprojekt wurde mit Hilfe des Grover-Algorithmus und einer Extrapolation der Daten auf eine praxisrelevante Modellgröße gezeigt, dass sich die Monte-Carlo-Rechenzeit von zehn Jahren mit herkömmlichen Rechnern auf weniger als 30 Minuten mit einem Quantencomputer reduzieren würde.

Portfoliooptimierung und Derivateberechnung profitieren

Ähnliche Erfolge zeichnen sich beim Einsatz von Quantencomputing bei der Portfoliooptimierung, der Vorhersage von Finanzkrisen, der Preisbestimmung von Finanzderivaten, bei Kreditbewertungsanpassungen oder bei der Arbitrage ab. Für Banken kann Arbitrage ein lohnendes Geschäft sein, da häufig kein Risiko gegeben ist und die Ausführung vollautomatisiert ist. Komplexe Arbitragestrategien sind nur beschränkt mit klassischen Computern umsetzbar. Auch die Betrugserkennung gehört zu den möglichen Anwendungen für Quantencomputing.

Banken mit eigener Forschung

Einige Banken haben Forschungsteams, die Quantenalgorithmen entwickeln. JP Morgan Chase, die ETH Zürich und IBM haben 2019 eine gemeinsame Forschungsarbeit veröffentlicht, in der ein Verfahren zur Preisbestimmung von Optionen auf einem IBM-Quantencomputer mit 20 Qubits durchgeführt wurde. Dafür wurde das Verfahren „Amplitude Amplification" statt der Monte-Carlo-Methode verwendet, eine Technik, die am Grover-Suchalgorithmus angelehnt ist. Tests auf einem realen Quantencomputer zeigten eine quadratische Rechenzeitverkürzung dieses Ansatzes gegenüber klassischen Methoden. Eine kommerzielle Nutzung der Methode ist mittelfristig zu erwarten.

> „Die Rechenzeit reduziert sich von zehn Jahren auf weniger als 30 Minuten."

Die spanische Bank BBVA hat einen vielversprechenden Ansatz für die Kreditneubewertung mit einem Quantenalgorithmus entwickelt. Auch hier wurde die übliche Monte-Carlo-Methode durch eine wirkungsvollere Berechnung ersetzt.

Einsatz in Versicherungen

Auch für Versicherungsunternehmen ergeben sich zahlreiche Anwendungsfälle und Nutzungsszenarien des Quantencomputings. Hier sticht der Bereich Risikomodellierung ebenfalls heraus. Riesige Datenmengen und komplexe Modelle können künftig in weit kürzerer Zeit als bisher verwertbare Ergebnisse liefern. »

Mögliche Einsatzszenarien sind beispielsweise die Realtime-Risikoaggregation im Underwriting oder die Modellierung von Supply-Chain-Störungen und damit verbundenen Risiken. Auch die schnelle Berechnung von Liability-Risiken oder die Simulation von Wettersystemen, um Katastrophen und damit assoziierte Risiken besser vorherzusehen und einzuschätzen, sind relevante Anwendungen.

Darüber hinaus bietet die schnelle Verarbeitung riesiger Datenmengen durch Quantencomputer weiteres Potenzial in den Servicebereichen von Versicherungen. Zu denken ist an die Optimierung individueller Customer Journeys, ein verbessertes Customer Relationship Management oder die Realtime-Automatisierung der Claims-Funktion. Auch ein wirksamerer Einsatz von Künstlicher Intelligenz ist möglich. Neue Geschäftsmodelle wie Insurance-on-Demand-Angebote und neue Varianten von Pay-as-you-live-Tarifen lassen sich aufgrund der höheren Leistungsfähigkeit von Quantencomputern einfacher umsetzen. Daraus ergeben sich entsprechende Wettbewerbsvorteile.

Neue Risiken durch die Technologie

Doch neben allen Chancen kann sich Quantencomputing auch als zusätzliches Risiko erweisen. Die Vorboten sind bereits am Horizont zu sehen. Zwar steht die neue Technologie erst am Anfang, doch IT-Sicherheitsexperten warnen bereits davor, dass klassische kryptographische Verfahren bedroht sind.

Gewiss ist bereits heute, dass Verschlüsselungsverfahren für das Onlinebanking, Prozesse bei Kartenzahlungen und Geldautomaten, aber auch Distributed-Ledger-Technologien, auf denen die Blockchain beruht, angepasst werden müssen, um das heutige Sicherheitsniveau in das Quantenzeitalter hinüberzuretten. Nach Auffassung des Bankenverbands hat der Einsatz von Quantencomputern Auswirkungen auf alle derzeit genutzten kryptographischen Verschlüsselungsverfahren. Speziell für Rückversicherer ist dieses Thema deshalb hochrelevant. Hinzu kommt, dass Fortschritte in der KI auch neuartige perfektionierte Cyber-Attacken ermöglichen.

> „Es gibt auch Potenzial in den Servicebereichen der Versicherer.“

Nicht nur ein Hype

Auch Quantencomputing wird wahrscheinlich den üblichen Hype-Zyklus von Innovationen durchlaufen. Deshalb besteht die Gefahr, dass die kurzfristigen Wirkungen der Technologie überschätzt werden. Es fehlt ja immer noch an praxisrelevanten Anwendungen. Nichtdestotrotz gilt es als sicher, dass die Finanzwirtschaft langfristig das Potenzial funktionierender Quantencomputer ausnutzen wird.

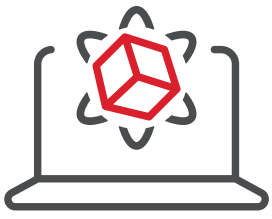
Finanzdienstleister, die heute erste Nutzungsszenarien identifizieren, in den Aufbau von Expertise und Infrastruktur investieren und eine Roadmap für die Nutzung von Quantencomputing planen, können zuversichtlicher auf die Entwicklung der kommenden Jahre schauen und sich bietende Wettbewerbsvorteile schneller nutzen.

Und: Quantencomputing kann als disruptive Technologie bestehende Branchen und Geschäftsmodelle ähnlich stark verändern wie klassische digitale Anwendungen. «

Matthias Frerichs
ist Senior Manager Banking bei Sopra Steria.
matthias.frerichs@soprasteria.com

Michael Maczan
ist Chief Technology Officer bei ISS Software.
michael.maczan@iss.soprasteria.com

kurz & knapp



Für **34 Prozent**
der Unternehmen und Verwaltungen ist die Simulation von Szenarien (etwa Finanzrisikomodelle) relevant.

Quelle: Potenzialanalyse „Quantencomputing“ (Sopra Steria), 2021

DENKANSTOSS

Evolution statt Revolution

Für die Ausbildung von Quantencomputing-Experten muss nicht alles neu erfunden werden. Prof. Dr. Helena Liebelt ist für einen der weltweit ersten Studiengänge für Quantencomputing an der TH Deggendorf verantwortlich. Das Masterstudium deckt auch das High Performance Computing ab, wie sie im Gespräch erklärt.

Zu einem der 30 Plätze im Masterstudium Quantencomputing der TH Deggendorf ist zugelassen, wer einen Bachelor in Informatik, Physik, Technik oder Ingenieurwesen vorweist und einen Einstellungstest besteht. Das Studium integriert auch das Thema High Performance Computing (HPC).

In dem auf drei Semester angelegten Masterstudium lernen die Studierenden, Programme für Hoch- und Höchstleistungsrechner zu entwickeln und Superrechner zu entwerfen. Parallel arbeitende Hochleistungsrechner und Rechencluster übernehmen heute schon Simulationen in der Meteorologie und Genetik, bei denen Einzelcomputer überfordert sind. Genau dies gehört auch zu den Anwendungen für Quantencomputer.

So gesehen ist Quantencomputing in Lehre und Ausbildung eine evolutionäre Weiterentwicklung, die auf HPC aufbaut. Der Nobelpreisträger Richard Feynman, der in den 1980er Jahren den Bau des ersten Quantencomputers vorgeschlagen hatte, stellte schon die Frage, ob Quantenphysik wirksam von klassischen Computern simuliert werden könne. Eine der Antworten darauf führt nach Deggendorf.

Studiengang startet

Dort wird ab Herbst 2021 das Design von Quantencomputern gelehrt, aber auch die Entwicklung von Anwendungen auf Basis von Programmiersprachen wie der von Google entwickelten Cirq, die bereits zu einer Art Standard in der Wissenschaft geworden ist, aber als Python-Bibliothek auch Wurzeln in der „alten" Welt hat. Auch nicht völlig neu ist das Projektmanagement bei der Entwicklung von Quantencomputing. Methoden wie agile Entwicklung, Scrum oder Kanban behalten ihre Gültigkeit.

© Nastassia Shestakova/Laukart Photography

Prof. Dr. Helena Liebelt
hat eine Professur für Informatik an der Technischen Hochschule Deggendorf.

> „Es wird einen Mangel an Quanten-Experten geben."

Es kommen neue Themen hinzu, die für die Entwicklung des Quantencomputings wichtig sind. Zum Beispiel ist „Energieeffizienz und Softwareoptimierung" einer der Schwerpunkte im Masterstudiengang. „Es wird aber", so Helena Liebelt, „auf längere Sicht noch eine Verbindung zwischen Quantencomputing und der traditionellen IT geben."

Rein rechnerisch werden Ende 2022 die ersten 30 Absolventinnen und Absolventen die TH Deggendorf mit einem Master verlassen. Das passt zur Ankündigung von IBM, 2023 einen Quantencomputer mit 1.000 Qubits auf den Markt zu bringen. Diese Zahl gilt als magische Grenze zur Lösung komplexer Probleme jenseits von Proof-of-Concept-Studien.

Sorgen um eine Anstellung müssen sich die Absolventen wohl nicht machen: Es wird auf längere Sicht einen Mangel an Quanten-Experten und naturgemäß eine Ballung dieser Fachkräfte bei einigen wenigen Unternehmen geben, die an Quantencomputing arbeiten. Dazu gehören IBM, Amazon, Google oder Microsoft sowie Großunternehmen etwa aus der Automobilindustrie. Die Master-Ausbildung in Deggendorf ist daher auch ein wichtiger Beitrag, um das Quantencomputing in die Breite zu tragen. «

Das Gespräch führte Thomas Pelkmann von Faktor 3.

THINK TANK

Quanten-computing als neue Bedrohung

Viele derzeitige kryptographische Verfahren sind bedroht, sobald es leistungsfähige Quantencomputer gibt. Im Hochsicherheitsbereich hat deshalb bereits die Migration zur Post-Quanten-Kryptographie begonnen, wie Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), im Interview berichtet.

Herr Schönbohm, ist Quantencomputing ein potenzielles Sicherheitsrisiko für Unternehmen und öffentliche Verwaltungen?
Ja, definitiv. Aber Quantentechnologien bieten mit Anwendungen wie der Quantum Key Distribution definitiv auch eine Chance.

Warum ist Quantencomputing gefährlich?
Viele kryptographische Verfahren beruhen auf der Annahme, dass gewisse mathematische Probleme schwer zu lösen sind. Das Standardbeispiel hierfür ist die Zerlegung einer sehr großen Zahl in ihre Primfaktoren. Hierbei handelt es um eine Annahme, die bisher weder bewiesen noch widerlegt werden konnte. Allerdings nur für herkömmliche Computertechnik. Leistungsstarke universelle Quantencomputer werden voraussichtlich dazu in der Lage sein, große Zahlen zu faktorisieren. Dies wurde schon Mitte der 1990er Jahre vom US-Informatiker Peter Shor gezeigt, indem er Quantenalgorithmen entwickelt hat, mit denen die beiden für die Kryptographie grundlegenden mathematischen Probleme gelöst werden können. Sobald Quantencomputing ausreichend skaliert, das heißt Quantencomputer gebaut werden, auf denen die Algorithmen von Shor für große Inputlängen implementiert werden können, sind die meisten der heute eingesetzten Verfahren zur Schlüsseleinigung und zur Authentisierung nicht mehr sicher.

Ab wann müssen Unternehmen mit einer erhöhten Bedrohung rechnen?
Das hängt vom Anwendungsfall ab. Gerade im Hochsicherheitsbereich müssen wir uns mit dem „Store now, decrypt later"-Szenario auseinandersetzen. In diesem Szenario wird verschlüsselte Kommunikation heute aufgezeichnet und könnte in Zukunft geknackt werden. Dies betrifft natürlich auch Unternehmen, die Informationen mit einer langen Lebensdauer und einem hohen Schutzbedarf verarbeiten. Hinsichtlich Signaturverfahren zur Authentisierung ist die Lage etwas entspannter. Signaturen müssen meist nur zum Zeitpunkt der Prüfung gültig sein. Allerdings werden Signaturschlüssel in mitunter langlebigen digitalen Zertifikaten an die Identität ihrer Besitzer gebunden. Daher ist auch für Signaturanwendungen ein rechtzeitiger Umstieg auf quantencomputerresistente Lösungen notwendig.

Wer sind die potenziellen Angreifer?
Stand heute kann man sagen, dass Quantencomputer auf absehbare Zeit kein Massenprodukt werden. Es gibt jedoch erste Angebote, „Quantencomputing as a Service" zu nutzen. Potenziell kann dieser Service für verschiedene, gegebenenfalls auch illegale Zwecke genutzt werden. Kryptographische Verfahren werden sich allerdings auch mit Quantencomputern nicht innerhalb von Sekunden brechen lassen. Als Cyber-Sicherheitsbehörde des Bundes haben wir dazu die Studie „Entwicklungsstand Quantencomputer" veröffentlicht. Allerdings sind Prognosen in diesem Bereich schwierig, denn sprunghafte Entwicklungen sind nicht auszuschließen.

Arne Schönbohm
ist Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

> „Potenziell kann Quantencomputing as a Service auch für illegale Zwecke genutzt werden.“

Wie unterstützt das BSI Unternehmen und Verwaltungen dabei, dem Sicherheitsrisiko zu begegnen?
Im Hochsicherheitsbereich hat das BSI die Migration zu Post-Quanten-Kryptographie begonnen. Darunter versteht man kryptographische Verfahren, von denen man annimmt, dass sie auch mit Quantencomputern nicht gebrochen werden können. Bereits jetzt steht im Kommunikationsbereich ein zum Schutz von Verschlusssachen bis zum Einstufungsgrad „Geheim“ zugelassenes Produkt zur Verfügung, das ein Post-Quanten-Verfahren zur Schlüsseleinigung umsetzt.

Aktuell haben wir zwei Projekte ausgeschrieben, um dem Sicherheitsrisiko durch Quantencomputing zu begegnen. Dabei geht es zum einen um die Integration von Post-Quanten-Verfahren in den E-Mail-Client Thunderbird, zum anderen soll die BSI-Kryptobibliothek aktualisiert und die BSI-Empfehlungen dort umgesetzt werden.

Neben der Post-Quanten-Kryptographie, die mathematische Lösungen für die Bedrohung durch Quantencomputing liefert, gibt es auch einen anderen Weg, dieser Bedrohung zu begegnen: die Quantenkryptographie oder Quantenkommunikation. Hierbei sollen kryptographische Schlüssel auf Basis von Prinzipien der Quantenmechanik sicher vereinbart werden – die Quantum Key Distribution (QKD). In gewisser Weise können sich Post-Quanten-Kryptographie und QKD ergänzen. Erst kürzlich wurde im Rahmen des Projektes QuNET eine sichere Videokonferenz zwischen BSI und BMBF demonstriert, die durch eine Kombination beider Verfahren hybrid gesichert war.

Gibt es weitere Sicherheitsinitiativen auf Bundes- und Europaebene?
Im Bereich Post-Quanten-Kryptographie gibt es eine Reihe von Projekten, die vom BMBF gefördert werden. Beispielweise beschäftigt sich das Projekt PQC4MED mit dem Schutz von Daten in der medizinischen Versorgung. Das Projekt QuaSiModO untersucht die Realisierung von quantensicheren virtuellen privaten Netzwerken (VPN). Im Bereich QKD ist neben dem bereits erwähnten Projekt QuNET insbesondere die europäische Initiative EuroQCI zum Aufbau einer europäischen Quantum Communication Infrastructure zu nennen, die auch eine Weltraumkomponente SAGA enthalten soll. Daneben gibt es eine Vielzahl von weiteren europäischen und deutschen Projekten, auch auf Länderebene.

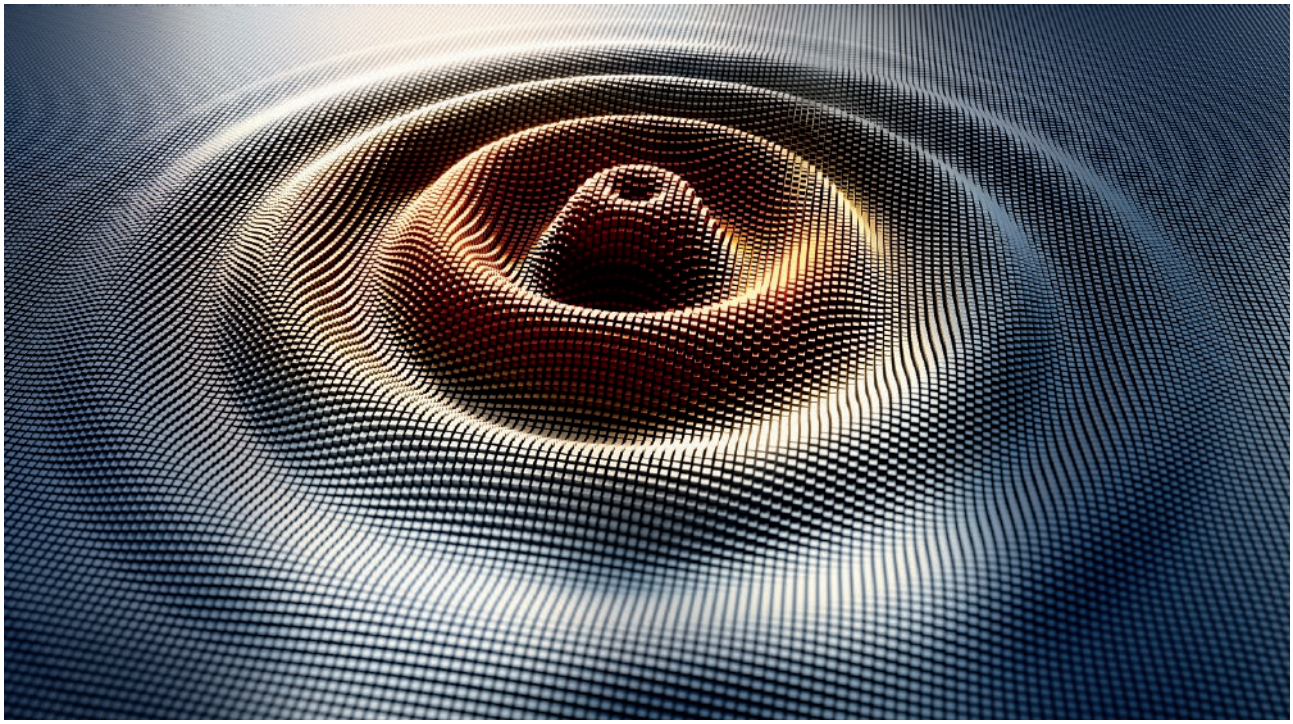
Kann Quantencomputing auf der anderen Seite auch die Datensicherheit erhöhen?
Ich bin mir sicher, dass Quantencomputing für Informationssicherheit nutzbar gemacht werden kann. Wann und wie, das können wir heute noch nicht absehen. Insgesamt ist es aber wichtig, heute schon bei der Ausbildung von Sicherheitsexpertinnen und -experten Quantencomputer zu berücksichtigen. «

Das Interview führte Eric Czotscher.

PRAXIS

Daten schützen. Jetzt!

Bis standardisierte Verfahren und praxistaugliche Technologien zum Schutz vor den Gefahren kryptographisch relevanter Quantencomputer bereitstehen, werden noch Jahre vergehen. Unternehmen und Verwaltungen können sich aber bereits heute schützen.



Quanteneffekte begründen nicht nur das Problem, langfristig liefern sie auch die Lösung.

Für Unternehmen, die vertrauliche Daten gar nicht oder ausschließlich lokal verarbeiten, ist die Bedrohung durch Quantencomputer eher gering. Unternehmen aber, die Daten übertragen, deren Vertraulichkeit auch noch in vielen Jahren gewährleistet sein muss, sollten jetzt schon aktiv werden.

Dies gilt vor allem dann, wenn die Datenübertragung über öffentliche Netze erfolgt und der Schutz auf asymmetrischen oder hybriden kryptographischen Verfahren basiert, was bei den meisten Kommunikationsprotokollen der Fall ist.

Datensparsamkeit beachten

Bei der Kommunikation über öffentliche Netze wie das Internet kann das Mitschneiden der Datenübertragung grundsätzlich nicht ausgeschlossen werden. Schon heute ist die Bedrohung real, dass ein Angreifer in den Besitz verschlüsselter Daten kommt und diese bei Verfügbarkeit leistungsfähiger Quantencomputer in der Zukunft entschlüsselt (store now, decrypt later).

Um diese Bedrohung zu begrenzen, gibt es einen einfachen Ansatz, der auch schon im Vor-Quanten-Zeitalter wirkungsvoll ist: Datenvermeidung und Datensparsamkeit. Insbesondere der Umfang der Übertragung vertraulicher Daten über öffentliche Netze sollte hinterfragt werden – auch bei einer Verschlüsselung. Strategien wie Outsourcing oder Cloud-Nutzung sollten in die Überlegungen einbezogen werden. Dazu gehört aber auch, Redundanzen in der Datenhaltung aufzulösen, die Speicherdauer zu begrenzen und sichere Löschverfahren zu verwenden.

Idealerweise kann die Kommunikation physisch von öffentlichen Netzen getrennt werden. Dies ist zum Beispiel bei der Verbindung von Standorten georedundanter Rechenzentren sinnvoll. Die öffentliche Verwaltung geht diesen Weg bereits mit der Einführung des Kerntransportnetzes Bund (KTN-Bund) als technischer Basis der Netze des Bundes. Dieses ist von der Technik öffentlicher oder kommerziell betriebener Netze unabhängig.

Hohe Hürden für Angreifer

Ein zweiter Ansatz ist, die Hürde für das Entschlüsseln von Daten möglichst hoch zu gestalten. Bei der Verwendung von Standardprodukten sollte man die Möglichkeiten für die Aktivierung und Konfiguration kryptographischer Funktionen voll ausschöpfen. Mehr Handlungsspielraum ergibt sich bei der Neu- und Weiterentwicklung eigener Anwendungen. Hier sollten kryptographische Mechanismen flexibel gestalten werden, um auf künftige Entwicklungen reagieren und nicht mehr wirksame Algorithmen austauschen zu können. Das BSI nennt dies „Kryptoagilität".

US-Standard für Post-Quanten-Kryptographie

Eine mittelfristige Lösung verspricht die Post-Quanten-Kryptographie. Quantenresistente Algorithmen werden auf klassischen IT-Plattformen implementiert und gründen ihre Sicherheit wie heutige Algorithmen auf mathematischer Komplexität. Nur die mathematischen Hürden sind andere: Das Problem diskreter Logarithmen oder der Zerlegung

> „Eine mittelfristige Lösung verspricht die Post-Quanten-Kryptographie."

sehr großer Zahlen in ihre Primfaktoren wird durch andere, auch für Quantencomputer schwer lösbare Probleme ersetzt, wie Fragen über Vektoren in Gittern, oder durch mathematische Methoden, die auch bei Fehlerkorrekturen verwendet werden.

Das amerikanische National Institute of Standards and Technology (NIST) führt derzeit einen Auswahlprozess durch, um Algorithmen zu identifizieren und zu standardisieren, die sowohl der Rechenleistung von Quantencomputern als auch derjenigen klassischer Computer standhalten können. Die Bekanntgabe der ersten Draft-Standards mit der Möglichkeit der öffentlichen Kommentierung ist für 2022/2023 geplant. 2024 könnte der neue Standard bereits erscheinen.

Parallel zu den Standardisierungstätigkeiten des NIST finden auch in Deutschland Vorbereitungen auf das Quanten-Zeitalter statt, unter anderem durch das BSI. Ein Beispiel für die Forschungstätigkeiten in Deutschland liefert die Technische Universität München (TUM). Ein Team der TUM hat erst kürzlich einen Computerchip entworfen, der Post-Quanten-Kryptographie sehr effizient umsetzt. Er basiert auf dem quelloffenen RISC-V-Standard.

Noch mehr Sicherheit durch Quantenkommunikation

Perspektivisch lassen sich Kommunikationsverbindungen direkt über Quantentechnologien absichern. In heutigen Kommunikationsprotokollen bieten die Elemente, die auf asymmetrischer Kryptographie beruhen, die wesentliche Angriffsfläche für Quantencomputer. Elementar ist hier die Schlüsselverteilung, denn Sender und Empfänger benötigen dieselben symmetrischen Schlüssel: ein begehrtes Gut für Angreifer. Eine grundlegende Beseitigung dieser Angriffsfläche verspricht die Quantenschlüsselverteilung (Quantum Key Distribution), die Quanteneffekte nutzt, um kryptographische Schlüssel mit spezieller Hardware zu erzeugen und zu verteilen. Hier wird Information in Form von Quantenzuständen ausgetauscht.

Wissenschaftliche Betrachtungen dazu ergaben, dass es physikalisch unmöglich ist, diese Art der Informationsübertragung und somit den Vorgang der Quantenschlüsselverteilung im Netzwerk zu belauschen, ohne dass die Kommunikationspartner dies erkennen. Angriffe scheitern somit nicht mangels Rechenleistung, sondern werden unmöglich – zumindest in der Theorie.

In Zukunft könnten Quantencomputer über Quantennetzwerke oder ein Quanteninternet Quantenzustände und somit Informationen austauschen. Über erste erfolgreiche Implementierungen wurde bereits in der Fachpresse berichtet. «

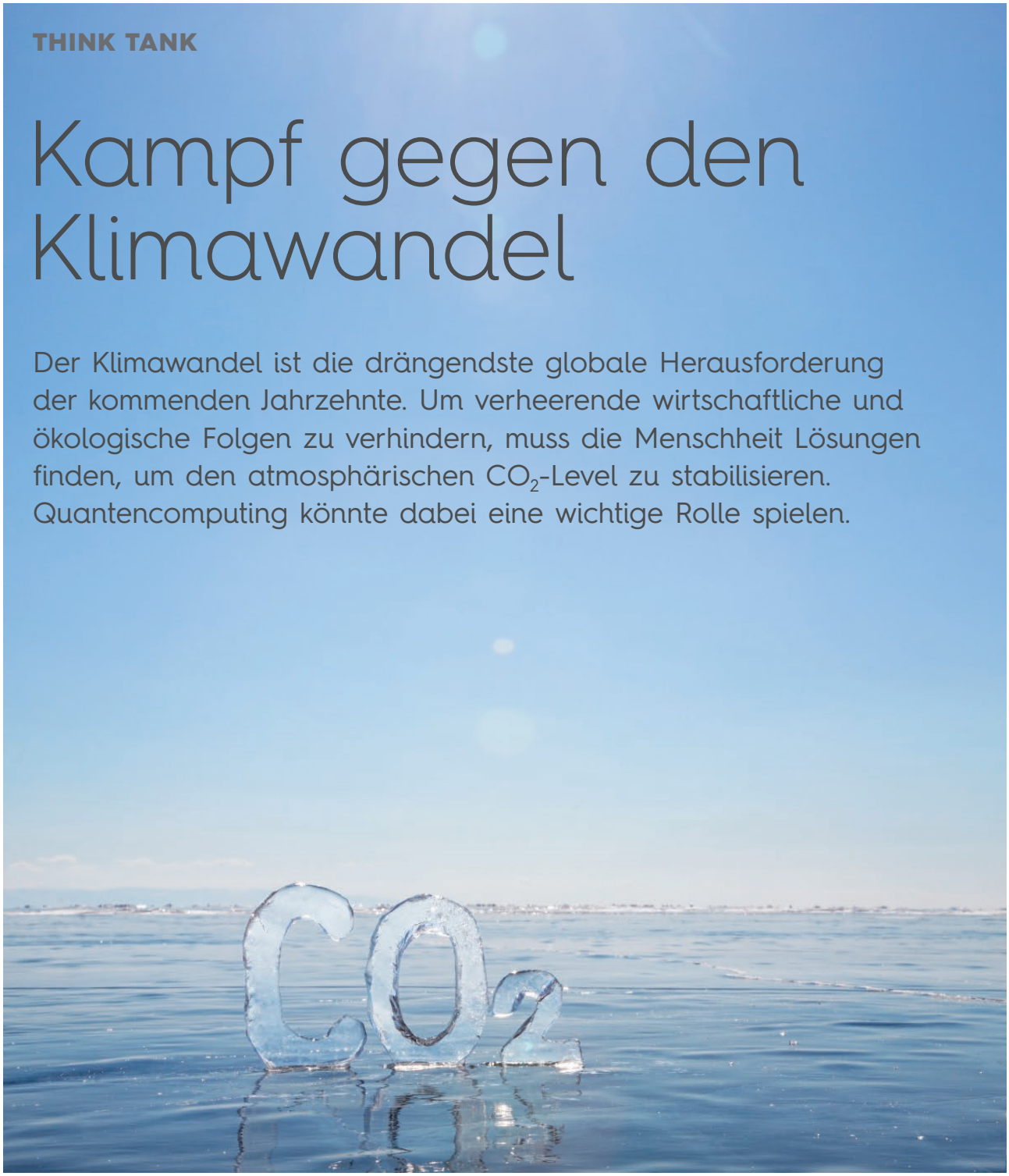
Alfred Weingärtner
ist Senior Consultant Cyber Security Public Sector bei Sopra Steria.
alfred.weingaertner@soprasteria.com

Eckart Begemann
ist Senior Consultant Cyber Security Public Sector bei Sopra Steria.
eckart.begemann@soprasteria.com

THINK TANK

Kampf gegen den Klimawandel

Der Klimawandel ist die drängendste globale Herausforderung der kommenden Jahrzehnte. Um verheerende wirtschaftliche und ökologische Folgen zu verhindern, muss die Menschheit Lösungen finden, um den atmosphärischen CO_2-Level zu stabilisieren. Quantencomputing könnte dabei eine wichtige Rolle spielen.



Der Forschungsaufwand, der in klimapositive Technologien investiert wird, ist schon heute sehr groß. Für einige dieser Ansätze könnte Quantencomputing künftig eine wichtige Rolle spielen. Insbesondere bei der Optimierung von chemischen Vorgängen wird ein großes Potenzial gesehen.

Dass chemische Vorgänge ökonomisch und gesellschaftlich hochrelevant sind, zeigt sich am Beispiel des Haber-Bosch-Verfahrens. Dieses im 20. Jahrhundert entwickelte Verfahren zur industriellen Ammoniaksynthese ist unerlässlich für die weltweite Düngerproduktion und ernährt indirekt etwa die Hälfte der Weltbevölkerung.

Ein wichtiger Teilschritt in der Entwicklung eines neuen chemischen Verfahrens ist die Optimierung des Katalysators, also des zentralen Moleküls, das die Reaktion beschleunigt. Dessen Erforschung geschieht

oft durch zeitintensive Laborarbeit, in der verschiedene Kandidaten hergestellt und inkrementell verbessert werden. Die Hoffnung ist, dass solche Optimierungsprozesse in Zukunft mit Hilfe von Quantencomputern beschleunigt werden können.

CO_2-Fixierung als Aufgabe

Ein Kandidat für eine chemische Reaktion, die in diesem Jahrhundert einen großen Stellenwert einnehmen könnte, ist die CO_2-Fixierung. Von Pflanzen wird diese bereits genutzt, um Zucker aus Kohlendioxid und Wasser herzustellen. Deshalb sind großflächige Waldgebiete wie der Amazonas effektive CO_2-Senken. Industriell könnte dieser Prozess dazu verwendet werden, um Biokraftstoffe wie Methanol aus CO_2 herzustellen. Entscheidend für eine wirtschaftliche Umsetzbarkeit ist aber auch hier, ob es gelingt, einen geeigneten Katalysator herzustellen, der die Reaktion unter günstigen Bedingungen effizient durchführt.

Technologieunternehmen forschen

Großunternehmen wie Microsoft, Google und IBM haben das Potenzial dieses Anwendungsgebiets bereits erkannt. Sie sind derzeit an der Entwicklung von Algorithmen beteiligt, die die Modellierung chemischer Reaktionen auf Quantencomputern ermöglichen.

Dabei setzen sie auf unterschiedliche Strategien: So fokussieren sich IBM und Google auf Verfahren, die auf bereits bestehenden Quantencomputern durchgeführt werden können. Diese Generation von Quantencomputern besitzt aber noch technologische Schwachstellen, die verbessert werden müssen. Dadurch liegen ihre momentanen Möglichkeiten, chemische Prozesse zu simulieren, noch deutlich hinter denen klassischer Computer. Sie werden aber stetig verbessert. Wichtige Erstsimulationen können allerdings bereits heute durchgeführt werden.

Microsoft setzt demgegenüber auf eine längerfristige Strategie, indem es Verfahren erforscht, die robuster sind und auf zukünftige Generationen von Quantencomputern zugeschnitten sind, bei denen Qubits zuverlässig vor Fehlern geschützt sind. Durch die bessere Qualität und Effizienz dieser Quantencomputer verspricht man sich größere Fortschritte in der Simulation chemischer Reaktionen. Gleichzeitig besteht eine größere Ungewissheit. Denn die noch benötigten technologischen Durchbrüche im Quantencomputing lassen sich schwer vorhersehen.

Beiden Strategien ist gemein, dass sie einen hybriden Ansatz benutzen, bei dem Quantencomputer nur für die Simulation des komplexesten Teilbereichs der Moleküle verwendet werden, während klassische Computer die nötigen Parameter liefern. Wenn Quantencomputer leistungsfähiger und robuster werden, kann der ihnen zugewiesene Bereich stetig vergrößert werden. Durch diesen Ansatz kann die Zeit bis zum Erscheinen hochentwickelter Quantencomputer überbrückt und sinnvoll genutzt werden.

> „Hybrider Ansatz dient als Brücke in die Zukunft des Quantencomputings.“

Zudem bieten diese Unternehmen bereits heute Cloud-Zugang zu Quantenhardware für Firmen und Forschende an, die dadurch eigene Simulationen auf vorhandenen Quantencomputern durchführen können. Somit entsteht eine Kundenbindung, die idealerweise bis in das Zeitalter des Quantencomputings hineinreicht.

Wettbewerb sorgt für Fortschritte

Der Wettbewerb um die Vormachtstellung in der quantencomputergestützten Modellierung chemischer Reaktionen hat in kurzer Zeit zu beachtlichen Fortschritten geführt. Schätzungen für die benötigte Dauer solcher Simulationen auf hochentwickelten Quantencomputern konnten von anfänglich mehreren Jahren auf einige Wochen bis Tage reduziert werden. Die dafür benötigte Leistungssteigerung bestehender Quantencomputer hängt aber stark von der Entwicklung verbesserter Quantenhardware ab.

Gelingen die nötigen technologischen Fortschritte in der Entwicklung von Quantencomputern, eröffnet dies neue Möglichkeiten der computergestützten Katalyseforschung. Kreative Ansätze beispielsweise für die CO_2-Fixierung können leichter erschlossen werden. Aber auch bestehende Prozesse wie das erwähnte Haber-Bosch-Verfahren, das für 1,4 Prozent des weltweiten CO_2-Ausstoßes verantwortlich ist, lassen sich vermutlich deutlich verbessern. Damit öffnet sich auch ein Fenster, um den Klimawandel abzubremsen. «

Vera von Burg
ist Doktorandin im Fachbereich Quantenchemie an der ETH Zürich.

managementkompass@faz-institut.de

BLICKWECHSEL

Mit Digital Annealing Quanteneffekte nutzen

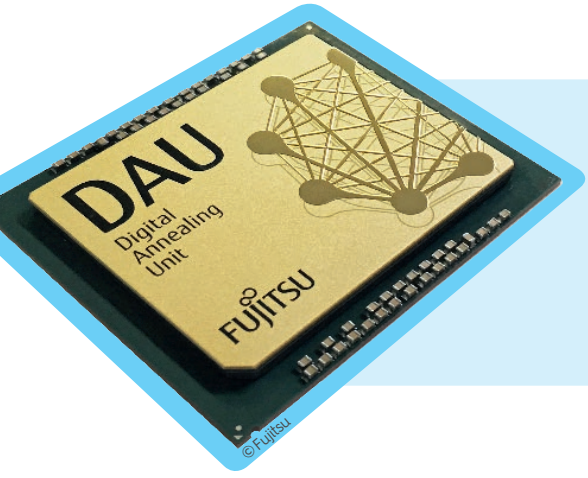
Ungeachtet aller Erfolgsmeldungen eignen sich heutige Quantenrechner noch kaum für den Einsatz in Unternehmen und Verwaltungen. Als Alternative bieten sich Brückentechnologien wie Digital Annealing an. Damit können Firmen erste Erfahrungen für das Quantencomputing sammeln. Mit der Technologie lassen sich Prozesse nahezu in Echtzeit optimieren.

Für Unternehmen, die ihre Effizienz steigern wollen, ist die Lösung kombinatorischer Optimierungsprobleme in Echtzeit derzeit noch eine Herausforderung. Da die benötigte Rechenleistung mit der Problemgröße exponentiell steigt, sind klassische IT-Architekturen dafür nur bedingt ausgelegt. Die theoretisch besser geeigneten Quantenrechner sind aber auf absehbare Zeit für die meisten Firmen nicht praktikabel einsetzbar. Denn um brauchbare Resultate liefern zu können, müssen sie auf Temperaturen nahe dem absoluten Nullpunkt heruntergekühlt und vor elektromagnetischer Strahlung abgeschirmt werden. Zudem benötigen sie einen Großteil ihrer Rechenleistung für die eigene Fehlerkorrektur – ein Aufwand, der für viele potenzielle Anwender nicht wirtschaftlich ist.

Erste Schritte in Richtung Quantencomputing

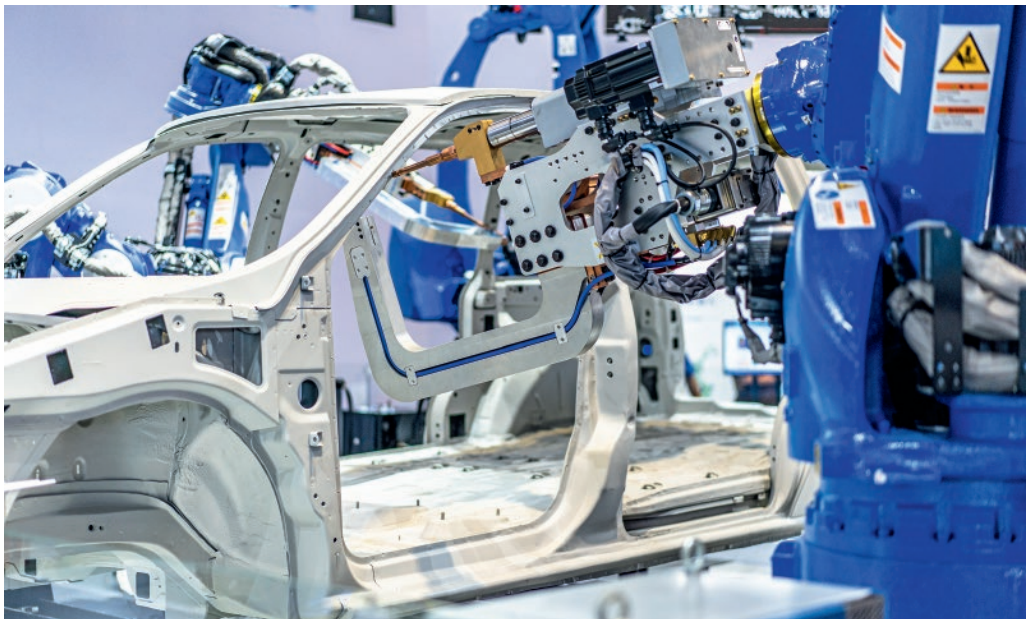
Dennoch ist es für Unternehmen sinnvoll, sich bereits heute auf die Ära des Quantencomputings vorzubereiten. Denn wenn die neue Technologie praktikabel nutzbar sein wird, werden diejenigen Firmen im Vorteil sein, die bereits Erfahrung damit haben. Die möglichen Einsatzbereiche sind vielfältig: Sie reichen von der Optimierung von Logistik- und Fertigungsprozessen über die Materialforschung in der Chemie und die Wirkstoffforschung in der Pharmaindustrie bis hin zu zu deutlich verbesserten Portfolio- und Risikoberechnungen in der Finanzindustrie.

Ein praktikabler Weg, um dieses Know-how zu erwerben und gleichzeitig bereits heute von deutlichen Prozessverbesserungen zu profitieren, ist der Einsatz von Brückentechnologien wie dem Digital Annealing. Dieses verwendet eine besondere Rechnerarchitektur, die zwar mit herkömmlicher Siliziumtechnologie umgesetzt wird, aber die Arbeitsweise eines Quantum Annealer nachbildet. Ein Quantum Annealer ist eine Variante eines „echten" Quantencomputers. Mit ihm lassen sich komplexe Berechnungen rund 10.000fach schneller durchführen als mit herkömmlichen IT-Systemen – sofern dies dort überhaupt umsetzbar ist.



DIGITAL ANNEALING

ist eine neue Technologie zur Lösung kombinatorischer Optimierungsprobleme in Echtzeit. Digital Annealing emuliert dafür die Eigenschaften von Qubits mit Hilfe klassischer Bits. In einem speziellen Chip ist jedes Bit mit jedem anderen Bit verbunden. Daher kann der Chip viele Rechenoperationen parallel ausführen – in Sekundenschnelle.



© THINK b – stock.adobe.com

Quantenrechner werden in Zukunft auch Industrieprozesse optimieren, beispielsweise das Schweißen per Roboter. Digital Annealing ermöglicht solche Optimierungen teils schon heute.

Anwendungsbeispiele

Bahn- und Hafenlogistik

In Deutschland nutzen Firmen unterschiedlicher Branchen die von Fujitsu entwickelte Digital-Annealing-Technologie. So setzt beispielsweise die Deutsche Bahn in einem Proof of Concept darauf, um Routen und Taktfrequenzen von Güterzügen zu optimieren. Bei etwa 700.000 Zugtrassen erfordert dies Optimierungsberechnungen mit einem hohen Komplexitätsgrad. Ein herkömmlicher Hochleistungsrechner benötigte dafür zwei Stunden, das Digital Annealing vier Minuten. Wichtig ist zudem die um rund 10 Prozent höhere Genauigkeit des quanteninspirierten Systems, was es ermöglicht, mehr Güterzüge auf die Strecke zu bringen.

Vor einer ähnlichen Herausforderung steht die Hamburg Port Authority (HPA). Sie optimiert mittels Digital Annealing die Verkehrssteuerung im Hamburger Hafen. Ziel ist, dass beim Löschen großer Containerschiffe der Abtransport der Container per Lkw so reibungslos wie möglich erfolgt. Dies lässt sich mit einer intelligenten Ampelsteuerung in Echtzeit erreichen, die zahlreiche aktuelle Informationen berücksichtigt. Dazu zählen etwa die Verkehrslage, die Art und Zahl der Fahrzeuge sowie deren Geschwindigkeit und Fahrstrecke.

Automobil- und Finanzindustrie

BMW wiederum hat das Digital Annealing eingesetzt, um die Bewegungen von Roboterarmen bei der Schweißnahtversiegelung zu optimieren. Mehrere Roboter arbeiten dabei parallel an einem Fahrzeug. Um den Vorgang zu beschleunigen, ließ der Automobilhersteller 1,8 × 10^{106} Varianten der Bewegungsabläufe analysieren, die beim Versiegeln von 64 Nähten anfallen. Das Ergebnis: Die Bewegungen der Roboterarme konnten um bis zu 40 Prozent reduziert werden. Die Berechnung dauerte außerdem nur etwa eine halbe Minute und war damit rund 17.000fach schneller als mit einem herkömmlichen IT-System. Ein weiteres Einsatzfeld ist der Finanzsektor. So hat main incubator, die F&E-Sparte der Commerzbank, einen Proof of Concept im Kreditportfolio-Management durchgeführt. Die Technologie ermöglicht es, Forderungen aus Leasing-Verträgen besser zu bündeln und das Liquiditätsmanagement zu verbessern.

> „Die Anwendung von Quanteneffekten ist keine Science Fiction mehr.“

Service per Cloud

Die Beispiele zeigen, dass mit Technologien wie dem Digital Annealing bereits heute massive Prozessverbesserungen möglich sind und die Anwendung von Quanteneffekten keine Science Fiction mehr ist. Dies gilt umso mehr, als dass die Technologie per Cloud-Service zur Verfügung steht. Unternehmen haben dadurch die Möglichkeit, sich ohne große Risiken und Kosten auf die Ära des Quantencomputings vorzubereiten und Wettbewerbsvorteile zu realisieren. «

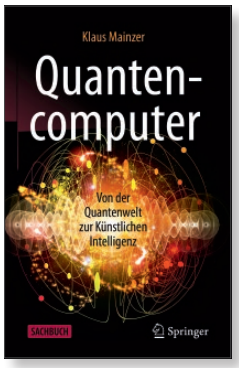
© Fujitsu

Dr. Joseph Reger
ist Fujitsu Fellow & Chief Technology Officer Central & Eastern Europe bei Fujitsu.

managementkompass@faz-institut.de

Buch & Web

FACHLITERATUR



Klaus Mainzer:
Quantencomputer: Von der Quantenwelt zur Künstlichen Intelligenz. Springer 2021

Die Grundlagen von Quantencomputing verständlich zu erklären – von den mathematischen und physikalischen Grundlagen bis zu den technischen Anwendungen – ist das Hauptziel dieses sehr empfehlenswerten Buchs. Tatsächlich werden alle wesentlichen Themen detailliert und mit Tiefgang dargestellt. Ganz ohne Mathematik geht es dabei nicht, aber auch mathematisch Unbegabte dürften sich in dem Buch zurechtfinden. Der Autor ist Experte für Künstliche Intelligenz und geht deshalb besonders darauf ein, wie stark KI von der Quantentechnologie profitieren kann. Dabei zeigt Mainzer auch die möglichen Gefahren für Mensch und Gesellschaft auf. Er plädiert dafür, möglichst bald in einen gesamtgesellschaftlichen Dialog über die Chancen und Risiken von KI und Quantencomputing einzutreten.

Anders Indset:
Quantenwirtschaft: Was kommt nach der Digitalisierung? Econ 2020

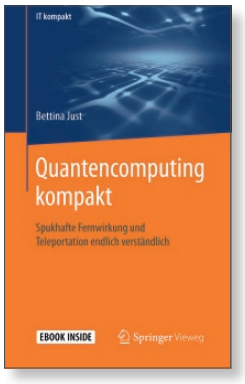
Der bekannte Wirtschaftsphilosoph Indset betrachtet die rasante Entwicklung von Künstlicher Intelligenz und den zukünftigen Verheißungen von Quantencomputing kritisch. Können menschliche Bedürfnisse tatsächlich von Computern erkannt und letztlich auch befriedigt werden? Wie stark werden Algorithmen in unseren Alltag eingreifen? Technologie wird nicht die Antwort auf alle Herausforderungen sein. Indset setzt sich für ein ganzheitlich orientiertes Denken, Planen und Wirtschaften ein, das über den bisher dominierenden, „kalten" Rationalismus hinausreicht. Den Begriff „Quantenwirtschaft" verwendet er in diesem Sinne als Metapher für eine neue, nachhaltigere Lebens- und Wirtschaftsweise, die auf Vernetzung beruht – analog zur Verschränkung der kleinsten atomaren Teilchen.

LINKS

» **https://www.quantentechnologien.de/**
Themenseite des BMBF zu den wichtigsten deutschen Quanten-Initiativen

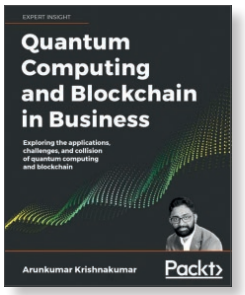
» **https://t1p.de/quantenfoerderung**
Überblick über Förderprogramme für Quantencomputing des BMWi

» **https://t1p.de/kryptographie**
Handlungsempfehlungen des BSI zur Migration in die Post-Quanten-Kryptographie



Bettina Just:
Quantencomputing kompakt. Spukhafte Fernwirkung und Teleportation endlich verständlich. Springer Vieweg 2021

Im Fokus dieser Einführung stehen die Algorithmen, mit denen auf Quantencomputern Rechnenoperationen durchgeführt werden. Die Funktionsweise dieser Quantenalgorithmen erläutert Just detailliert mit Hilfe von Modellen und Abbildungen sowie anhand konkreter Rechenbeispiele. Wer Quantencomputing wirklich verstehen will, kommt letztlich um die Mathematik der Quantenmechanik nicht herum. Die Autorin bietet hierfür einen denkbar einfachen Einstieg ohne höhere Mathematik. Interessant sind auch ihre Ausführungen zu den Systemeigenschaften von Quantencomputern. Da Qubits sich über die Quantenverschränkung gegenseitig beeinflussen, arbeitet ein Quantenschaltkreis wie ein selbstorganisierendes System. Aus diesem Grund lassen sich Quantenalgorithmen auch dazu verwenden, das Verhalten komplexer Systeme zu simulieren. Die Quantenschaltkreise schwingen sich regelrecht in eine Aufgabe ein und finden die Lösung durch die natürliche Wirksamkeit der Quanteneffekte.



Arunkumar Krishnakumar:
Quantum Computing and Blockchain in Business: Exploring the applications, challenges, and collision of quantum computing and blockchain.
Packt 2020 (Englisch)

Das Buch nimmt die beiden Technologien Distributed Ledger und Quantum Computing unter die Lupe und prüft, welche neuen Geschäftsmodelle und Anwendungen sich für Unternehmen und Verwaltungen daraus ergeben können. Krishnakumar ist Investor bei einem Venture-Capital-Unternehmen sowie Fintech-Blogger und hat einen guten Blick für die geschäftlichen Chancen neuer Technologien. Im ersten Teil des Buchs erläutert er zunächst anschaulich die Besonderheiten beider Technologien. Im zweiten Teil stellt er mögliche Praxisanwendungen vor, insbesondere aus der Finanzbranche, der öffentlichen Verwaltung, der chemischen Industrie sowie für Pharma und Medizin. Er geht detailliert auf Sicherheitsthemen ein und zeigt, welche Distributed-Ledger-Technologie als „Post-Quantum-Blockchain" auch dem Angriff von Quantencomputing standhalten kann. Interviews mit Forschern und Praktikern runden das Buch ab.

Glossar

» Atomfalle
Technik zum Einfangen neutraler Atome bei Tiefsttemperaturen, um mit ihnen beispielsweise Operationen für das Quantencomputing durchzuführen.

» Adiabatischer Quantencomputer
Spezieller Quantencomputer für Optimierungsaufgaben (auch: Quantum Annealing). Vereinfacht geht es um die Frage, wie eine Ressource optimal genutzt werden kann. Der adiabatische Quantencomputer führt keine mathematischen Berechnungen im klassischen Sinne durch. Das Optimum einer Rechengröße wird vielmehr mit dem Minimum der Energie eines Quantensystems identifiziert, in dessen innerer Struktur die Optimierungsaufgabe angelegt ist.

» Digital Annealing
Technologie zur Lösung kombinatorischer Optimierungsprobleme in Echtzeit. In einem speziell dafür entwickelten Chip ist jedes Bit mit jedem anderen Bit verbunden. Daher kann der Chip viele Rechenoperationen sehr schnell parallel ausführen. Digital Annealing wurde durch Quantenphänomene inspiriert, ist aber kein Quantencomputing.

» Distributed-Ledger-Technologie (DLT)
Dezentrale Datenbank, bei der die Daten und Transaktionen bei jedem Teilnehmer im Netzwerk redundant verschlüsselt gespeichert werden. Die Konsistenz und Richtigkeit der Teilnehmerdaten wird durch einen Konsensalgorithmus sichergestellt. Das Löschen von Daten ist nicht vorgesehen, weshalb personenbezogene Daten nicht gespeichert werden sollten. Die Blockchain basiert auf DLT.

» Grover-Algorithmus
Quantenalgorithmus zur Suche in unsortierten Datenbanken.

» Ionenfalle
In einer Ionenfalle werden Ionen, also elektrisch geladene Atome oder Moleküle, mittels elektrischer und magnetischer Felder festgehalten, um sie etwa für Operationen im Quantencomputing einzusetzen.

» Machine Learning
Computersystem, das selbständig lernt, Probleme zu lösen. Dafür wird das System befähigt, aus einer Vielzahl von Daten Muster zu erkennen. Danach kann es auch unbekannte Daten beurteilen.

» Post-Quantenkryptographie
Kryptographische Verfahren, von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht zu brechen sind. Im Gegensatz zur Quantenkryptographie werden diese Verfahren auf klassischer Hardware implementiert.

» Quantencomputing
Quantencomputer arbeiten mit Qubits. Ein Qubit kann im Zustand 0 oder 1 sein, es kann aber durch Überlagerung (Superposition) auch fast beliebige Mischzustände annehmen. Diese bilden ein mehrdimensionales Kontinuum zwischen 0 und 1. Dadurch lassen sich deutlich mehr Informationen speichen. Werden mehrere Qubits miteinander verkoppelt, steigt die Zahl der möglichen Kombinationen exponentiell und damit die Rechenleistung.

» Quanteneffekte
In der Welt der Quanten lassen sich Effekte beobachten, die mit der klassischen Physik nicht erklärbar sind: Licht kann als Teilchen oder als Welle auftreten; Ort und Geschwindigkeit eines Teilchens lassen sich nicht gleichzeitig beliebig genau messen. Einzelne Teilchen verhalten sich nicht deterministisch, in der Masse folgen sie aber statistischen Vorhersagen. Teilchen können auch miteinander verschränkt sein, das heißt, unabhängige, räumlich getrennte Teilchen tauschen untereinander ohne Zeitverzögerung Informationen über Ihren Zustand aus. Die verschränkten Teilchen befinden sich damit in einem definierten Zustand.

» Quantenkommunikation
Übertragung von Quantenzuständen über eine räumliche Distanz. Die Anwendungsmöglichkeiten reichen vom sicheren Schlüsselaustausch bis zur Skalierung von Rechenleistung durch den Zusammenschluss mehrerer räumlich getrennter Quantencomputer.

» Quantenkryptographie
Einsatz quantenmechanischer Effekte zur Datenverschlüsselung. Dazu gehört etwa der Austausch von Schlüsseln. Wenn dieser über einen Quantenkanal erfolgt, kann ein Dritter eine laufende Nachricht nicht abhören, ohne dass sich diese verändert.

» Quantenbit (Qubit)
Elementare Rechen- und Speichereinheit eines Quantencomputers.

» Store now, decrypt later
Angreifer können heute verschlüsselte Daten erbeuten, die sie aber erst in Zukunft etwa mit Hilfe von Quantencomputing entschlüsseln.

» Supraleiter
Materialien, deren Widerstand beim Unterschreiten einer bestimmten Temperatur gegen null geht.

» Universeller Quantencomputer
Ein Universal-Gate-Quantencomputer eignet sich für algorithmische Aufgaben beliebiger Komplexität und Art. Dafür müssen Algorithmen entwickelt werden, die Quanteneffekte nutzen.

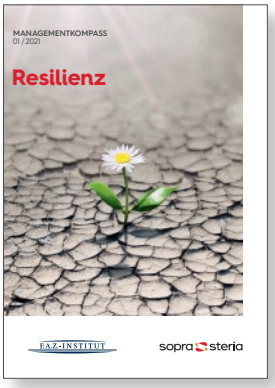
Aktuelle Studien

Managementkompass
Organisation x.0

Die Digitalisierung verändert die Art und Weise, wie sich Unternehmen und Verwaltungen organisieren. Die Pandemie hat bestehende Abläufe auf den Kopf gestellt. Fragen, die heute beantwortet werden müssen, sind: Wie hierarchisch soll unsere Organisation sein? Wie orts- und zeitflexibel können wir arbeiten? Denken wir noch in klassischen Büros oder wollen wir wortwörtlich Wände einreißen? Es gilt, Antworten zu finden, die sowohl dem eigenen Geschäftsmodell als auch den sich verändernden Ansprüchen der Beschäftigten entsprechen.

Managementkompass
Resilienz

Rasche Veränderungen und Ungewissheit prägen die Märkte nicht erst seit der Covid-19-Pandemie. Sowohl der technologische Fortschritt als auch kleine und große Krisen beeinflussen die Grundstruktur von Wirtschaft und Verwaltung. Organisationen müssen deshalb resilienter werden, um den Wandel nicht nur abzufedern, sondern um frühzeitig neue Chancen wahrzunehmen. Der Managementkompass zeigt mit Praxisbeispielen, wie sich die Resilienz erhöhen lässt.



Branchenkompass
Insurance

Befragung von 108 Führungskräften von Versicherungsgesellschaften und Vermittlungsunternehmen in Deutschland zu den aktuellen Herausforderungen und Trends der Branche. Der Branchenkompass enthält zudem drei Experteninterviews: mit Michael Diener (Vorstandsmitglied der Neuen Rechtsschutz-Versicherungsgesellschaft AG NRV), Guido Leber (Bereichsleiter für Konzern- und Unternehmensstrategie der ALH Gruppe) und Dr. Matthias Uebing (Gründer und Vorstand der mailo Versicherung AG).

IMPRESSUM

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts sowie für zwischenzeitliche Änderungen übernehmen Redaktion, Verlag und Herausgeber keine Gewähr.

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Frankenallee 71–81, 60327 Frankfurt am Main

Verlag: F.A.Z. BUSINESS MEDIA GmbH – Ein Unternehmen der F.A.Z.-Gruppe
Frankenallee 71–81, 60327 Frankfurt am Main
Geschäftsführung: Dominik Heyer, Hannes Ludwig

ISBN: 978-3-948353-36-0

Titelfoto: DP – stock.adobe.com

Redaktion: Eric Czotscher, Thilo Kampffmeyer, Jacqueline Preußer
Gestaltung und Satz: Christine Lambert
Lektorat: Juliane Streicher

Genderhinweis: Wir streben an, gut lesbare Texte zu veröffentlichen und dennoch in unseren Texten alle Geschlechter abzubilden. Das kann durch Nennung des generischen Maskulinums, Nennung beider Formen („Unternehmerinnen und Unternehmer" bzw. „Unternehmer/-innen") oder die Nutzung von neutralen Formulierungen („Studierende") geschehen. Bei allen Formen sind selbstverständlich immer alle Geschlechtergruppen gemeint – ohne jede Einschränkung. Von sprachlichen Sonderformen und -zeichen sehen wir ab.

Druck und Verarbeitung:
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6, 60386 Frankfurt am Main
www.zarbock.de

Mit Ökofarben auf umweltfreundlichem Papier gedruckt.
Diese Studie wurde klimaneutral hergestellt. Der CO_2-Ausstoß wurde durch Klimaschutzprojekte kompensiert.

klimaneutral
natureOffice.com | DE-644-419329
gedruckt

Ansprechpartner

Sopra Steria SE
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 22703-5219
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Frankenallee 71–81
60327 Frankfurt am Main
Telefon: (069) 7591-1961
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-948353-36-0

F.A.Z.-INSTITUT

sopra steria